Attorney Docket No. 1793.1176

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:

Chul-min KIM et al.

Application No.: Unassigned | Group Art Unit: Unassigned

Filed: February 6, 2004 | Examiner: Unassigned

For: APPARATUS AND METHOD OF ENCIPHERING DATA PACKET OF VARIABLE WIDTH

SUBMISSION OF CERTIFIED COPY OF PRIOR FOREIGN APPLICATION IN ACCORDANCE WITH THE REQUIREMENTS OF 37 C.F.R. § 1.55

Commissioner for Patents
PO Box 1450
Alexandria, VA 22313-1450

Sir:

In accordance with the provisions of 37 C.F.R. § 1.55, the applicants submit herewith a certified copy of the following foreign application:

Korean Patent Application No. 2003-7436
Filed: February 6, 2003

It is respectfully requested that the applicants be given the benefit of the foreign filing date as evidenced by the certified papers attached hereto, in accordance with the requirements of 35 U.S.C. § 119.

Respectfully submitted,
STAAS & HALSEY LLP

Date: February 6, 2004 By: _____
Michael D. Stein
Registration No. 37,240

1201 New York Ave, N.W., Suite 700
Washington, D.C. 20005
Telephone: (202) 434-1500
Facsimile: (202) 434-1501

대 한 민 국 특 허 청
KOREAN INTELLECTUAL PROPERTY OFFICE

별첨 사본은 아래 출원의 원본과 동일함을 증명함.

This is to certify that the following application annexed hereto is a true copy from the records of the Korean Intellectual Property Office.

출 원 번 호 : 10-2003-0007436
Application Number

출 원 년 월 일 : 2003년 02월 06일
Date of Application FEB 06, 2003

출 원 인 : 삼성전자주식회사
Applicant(s) SAMSUNG ELECTRONICS CO., LTD.

2004 년 01 월 15 일

특 허 청
COMMISSIONER

【서지사항】

【서류명】	특허출원서
【권리구분】	특허
【수신처】	특허청장
【참조번호】	0002
【제출일자】	2003.02.06
【국제특허분류】	H04L
【발명의 명칭】	가변 폭의 데이터 패킷을 암호화하는 장치 및 방법
【발명의 영문명칭】	Apparatus and method for enciphering a data packet of variable width
【출원인】	
【명칭】	삼성전자 주식회사
【출원인코드】	1-1998-104271-3
【대리인】	
【성명】	이영필
【대리인코드】	9-1998-000334-6
【포괄위임등록번호】	2003-003435-0
【대리인】	
【성명】	이해영
【대리인코드】	9-1999-000227-4
【포괄위임등록번호】	2003-003436-7
【발명자】	
【성명의 국문표기】	김철민
【성명의 영문표기】	KIM,Chul Min
【주민등록번호】	730701-1009314
【우편번호】	441-230
【주소】	경기도 수원시 권선구 평동 동남아파트 107동 603호
【국적】	KR
【발명자】	
【성명의 국문표기】	추교신
【성명의 영문표기】	CHOO,Kyo Shin
【주민등록번호】	760823-1520318

【우편번호】	449-844
【주소】	경기도 용인시 수지읍 성복리 84 강남아파트 106동 101호
【국적】	KR
【심사청구】	청구
【취지】	특허법 제42조의 규정에 의한 출원, 특허법 제60조의 규정에 의한 출원심사 를 청구합니다. 대리인 이영필 (인) 대리인 이해영 (인)
【수수료】	
【기본출원료】	20 면 29,000 원
【가산출원료】	45 면 45,000 원
【우선권주장료】	0 건 0 원
【심사청구료】	45 항 1,549,000 원
【합계】	1,623,000 원
【첨부서류】	1. 요약서·명세서(도면)_1통

【요약서】

【요약】

본 발명은 IPSEC을 따르는 암/복호화하는 장치 및 방법에 관한 것으로, 본 발명에 따른 가변 폭 데이터 패킷 암호화 장치는 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 고정 폭의 데이터 패킷을 생성하여 출력하는 가변 폭-고정 폭 데이터 패킷 변환부; 및 가변 폭-고정 폭 데이터 패킷 변환부에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 암호화부로 구성된다.

본 발명에 따르면, IPSEC 칩에 연결되는 외부 인터페이스 모듈이 변경된 경우, 임의의 외부 인터페이스 모듈로부터 출력되는 가변 폭의 데이터 패킷을 암호화하고, 가변 폭의 암호화 데이터 패킷을 복호화할 수 있다는 효과가 있다.

【대표도】

도 7

【명세서】

【발명의 명칭】

가변 폭의 데이터 패킷을 암호화하는 장치 및 방법 {Apparatus and method for enciphering a data packet of variable width}

【도면의 간단한 설명】

도 1은 종래의 IPSEC 암/복호화 장치의 구성도이다.

도 2는 본 발명의 일 실시예에 따른 가변 폭 데이터 패킷 암호화 장치의 구성도이다.

도 3은 상기 도 2의 암호화부(22)의 상세 구성도이다.

도 4는 본 발명의 일 실시예에 따른 가변 폭 암호화 데이터 패킷 복호화 장치의 구성도이다.

도 5는 상기 도 4의 복호화부(42)의 상세 구성도이다.

도 6은 본 발명을 적용한 IPSEC 암/복호화 장치의 일 예를 보여주는 도면이다.

도 7은 본 발명의 일 실시예에 따른 가변 폭-고정 폭 데이터 패킷 변환 장치의 구성도이다.

도 8은 상기 도 7의 가변 폭 데이터 패킷 결합부의 상세 구성도이다.

도 9는 상기 도 7의 고정 폭 데이터 패킷 결합부의 상세 구성도이다.

도 10은 본 발명의 일 실시예에 따른 가변 폭 데이터 패킷 암호화 방법의 흐름도이다.

도 11은 상기 도 10의 104 단계, 109 단계의 상세 흐름도이다.

도 12는 본 발명의 일 실시예에 따른 가변 폭 암호화 데이터 패킷 복호화 방법의 흐름도이다.

도 13은 상기 도 12의 124 단계, 129 단계의 상세 흐름도이다.

도 14는 본 발명의 일 실시예에 다른 가변 폭-고정 폭 데이터 패킷 변환 방법의 흐름도이다.

도 15는 상기 도 14의 143 단계의 상세 흐름도이다.

도 16은 상기 도 14의 1412 단계의 상세 흐름도이다.

【발명의 상세한 설명】

【발명의 목적】

【발명이 속하는 기술분야 및 그 분야의 종래기술】

<17> 본 발명은 IPSEC을 따르는 암/복호화하는 장치 및 방법에 관한 것이다.

<18> 도 1은 종래의 IPSEC 암/복호화 장치의 구성도이다

<19> 종래의 IPSEC(IP Security protocol) 암/복호화 장치는 메모리 컨트롤러(11), 패킷 제어부(12), ESP 메모리(13), ESP 엔진(14), AH 메모리(15), AH 엔진(16), 및 출력 메모리(17)로 구성된다.

<20> IPSEC(IP security protocol)은 인터넷 상에서 안전한 통신을 실현하기 위한 보안 규약이다. IPSEC은 특히, IP 계층의 보안을 위한 것으로, 가상 사설 네트워크(VPN, Virtual Private Network) 구현에 가장 널리 사용되는 기술이다. 즉, IPSEC은 가상 사설 네트워크에서 데이터가 도청당하는 것을 방지하기 위한 보

안 규약이다. IPSEC은 IP 헤더를 포함하는 전체 데이터 패킷에 대한 인증 기능을 제공하는 AH(Authentication Header), IP 헤더를 제외한 페이로드에 대한 암호화/인증 기능을 제공하는 ESP(Encapsulating Security Payload) 헤더, 및 AH/ESP를 포함한 각종 인터넷 보안 서비스에 필요한 SA 협상(Security Association Negotiation) 및 키 관리(Key Management)를 담당하는 ISAKMP/IKE(Internet Security Association and Key Management Protocol/Internet Key Exchange)로 구성된다.

<21> IPSEC은 사용자 단말기에 탑재되어, 특정 단말기들간에만 데이터를 주고받을 수 있게 해준다. IPSEC 표준안(RFC2401-2410)은 암/복호화나 인증 방식을 한 가지로 규정하지 않고, 여러 가지 방식의 암/복호화나 인증을 통제하기 위한 틀을 규정하고 있는데, 이 틀을 SA(security association)라 한다. 여러 가지 방식의 암/복호화나 인증의 알고리즘을 수행하기 위한 연산을 하드웨어(IPSEC on Chip)로 구현하면, 리소스 및 연산 시간을 상당히 단축시킬 수 있다.

<22> IPSEC을 하드웨어로 구현한 것이, 도 1에 도시된 IPSEC 암/복호화 장치이다. 메모리 컨트롤러(11)는 외부 인터페이스 모듈과 패킷 프로세서(12), 내부 메모리(ESP 메모리(13), AH 메모리(15), 출력 메모리(17))를 연동시킨다. 패킷 프로세서(12)는 메모리 컨트롤러와 IPSEC 엔진(ESP 엔진(14), AH 엔진(16))을 연동시킨다. IPSEC 엔진(ESP 엔진(14), AH 엔진(16))은 직접 외부 인터페이스 모듈로부터 데이터 패킷을 입력받지 않고, 내부의 메모리 컨트롤러를 통해, 데이터 패킷을 ESP 메모리(13), AH 메모리(15)에 저장한 후, IPSEC 엔진(ESP 엔진(14), AH 엔진(16))을 구동하는 방식을 사용한다. 출력 메모리(17)는 IPSEC 엔진(ESP 엔진(14), AH 엔진(16))에서 출력된 데이터 패킷을 저장한다.

<23> 상기와 같은 하드웨어적인 구현은 내부 동작과 함께 외부 인터페이스 모듈과의 인터페이스가 매우 중요한데, 외부 인터페이스 모듈이 미리 결정되어 있기 때문에, IPSEC 칩에서는 입

출력 포트 수가 미리 결정되어 있다. 따라서, 도시된 IPSEC 암/복호화 장치는 내부 시스템으로부터 데이터 폭이 고정된, 고정 폭의 데이터 패킷(예를 들면, 16 비트 데이터 패킷)을 입력받아, 암호화하여, 고정 폭의 암호화 데이터 패킷을 출력한다. 또는, 네트워크로부터 고정 폭의 암호화 데이터 패킷을 입력받아, 복호화하여, 고정 폭의 데이터 패킷을 출력한다.

<24> 종래에는 외부 인터페이스 모듈이 변경된 경우, 입출력 포트 수가 달라지게 되어, 메모리 컨트롤러를 다시 설계하여야 한다는 문제가 있었다. 즉, 메모리 컨트롤러 자체를 RTL(Register Transfer Language) 코드 수준에서부터 다시 설계해야 하는 불편함과 낭비를 초래하는 문제가 있었다. 특히, IPv6 환경에서는 IPv4 환경과는 달리, 특성상 다양한 플랫폼(예를 들면, 가정내의 모든 가전기기)에서 구동되어야 할 것이므로, 외부 인터페이스 모듈의 변경이 빈번하게 발생할 것이다.

【발명이 이루고자 하는 기술적 과제】

<25> 본 발명이 이루고자 하는 기술적 과제는 IPSEC 칩에 연결되는 외부 인터페이스 모듈이 변경된 경우, 임의의 외부 인터페이스 모듈로부터 출력되는 가변 폭의 데이터 패킷을 암호화하고, 가변 폭의 암호화 데이터 패킷을 복호화할 수 있는 장치 및 방법을 제공하는데 있다.

【발명의 구성 및 작용】

<26> 상기 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭 데이터 패킷 암호화 장치는 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 데이터 패킷을 생성하여

출력하는 가변 폭-고정 폭 데이터 패킷 변환부; 및 상기 가변 폭-고정 폭 데이터 패킷 변환부에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 암호화부로 구성된다.

<27> 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭 암호화 데이터 패킷 복호화 장치는 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 가변 폭-고정 폭 암호화 데이터 패킷 변환부; 및 상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부에서 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 복호화부로 구성된다.

<28> 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭-고정 폭 데이터 패킷 변환 장치는 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는 가변 폭 데이터 패킷 입출력부; 상기 가변 폭 데이터 패킷 입출력부에 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 상기 고정 폭의 제 1 데이터 패킷을 생성하는 가변 폭 데이터 패킷 결합부; 및 상기 가변 폭 데이터 패킷 결합부에서 생성된 고정 폭의 제 1 데이터 패킷을 출력하는 고정 폭 데이터 패킷 입출력부로 구성된다.

<29> 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭 데이터 패킷 암호화 방법은 (a) 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 단계; 및 (b) 상기 (a) 단계에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 단계로 구성된다.

<30> 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭 암호화 데이터 패킷 복호화 방법은 (a) 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 단계; 및 (b) 상기 (a) 단계에서 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 단계로 구성된다.

<31> 상기 또 다른 기술적 과제를 해결하기 위한 본 발명에 따른 가변 폭-고정 폭 데이터 패킷 변환 방법은 (a) 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는 단계; (b) 상기 (a) 단계에서 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 상기

고정 폭의 제 1 데이터 패킷을 생성하는 단계; 및 (c) 상기 (b1) 단계에서 생성된 고정 폭의 제 1 데이터 패킷을 출력하는 단계로 구성된다.

<32> 이하에서는 도면을 참조하여 본 발명의 바람직한 실시예들을 상세히 설명한다.

<33> 도 2는 본 발명의 일 실시예에 따른 가변 폭 데이터 패킷 암호화 장치의 구성도이다.

<34> 가변 폭 데이터 패킷 암호화 장치는 가변 폭-고정 폭 데이터 패킷 변환부(21) 및 암호화부(22)로 구성된다.

<35> 가변 폭-고정 폭 데이터 패킷 변환부(21)는 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 고정 폭의 데이터 패킷을 생성하여 출력한다. 예를 들어, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷(외부로 나가는 데이터 패킷)의 폭이 16 비트이고, 가변 폭 데이터 패킷 암호화 장치의 암호화 과정에서 처리되는 데이터 패킷의 폭이 32 비트인 경우, 즉, 가변 폭이 16 비트이고, 고정 폭이 32 비트인 경우, 가변 폭 데이터 패킷 암호화 장치는 데이터 폭이 32 비트인 데이터 패킷만을 처리할 수 있기 때문에, 내부 시스템으로부터 입력된 16 비트 데이터 패킷을 암호화할 수 없다. 따라서, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 두 개의 16 비트 데이터 패킷들을 차례로 입력받고, 입력받은 두 개의 16 비트 데이터 패킷들을 결합하여, 32 비트 데이터 패킷을 만들고, 이 32 비트 데이터 패킷을 암호화한다. 여기에서, 결합 값은 2이다. 만약, 외부 인터페이스 모듈로부터 입력되는 데이터 패킷의 폭이 8비트인 경우라면, 네 개를 차례로 입력받아, 처리하면 될 것이다. 이 경우, 결합 값은 4가 될 것이다. 가변 폭-고정 폭 데이터 패킷 변환부(21)는 암호화부(22)에서 암호화가 완료된 경우, 한 데이터 패킷씩 암호

화부(22)로 출력하므로, 종래의 메모리 콘트롤러와 패킷 프로세서의 역할을 동시에 담당한다.

<36> 암호화부(22)는 가변 폭-고정 폭 데이터 패킷 변환부(21)에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 고정 폭의 암호화 데이터 패킷을 생성하여 출력한다. 암호화부(22)에는 ESP 메모리, AH 메모리, IPSEC 엔진의 출력 데이터, 즉, 암호화된 데이터 패킷이 저장되는 메모리가 있다. 메모리의 경우, 입출력되는 데이터의 폭이 고정되어 있기 때문에, 암호화부(22)는 하나의 데이터 폭에 대해서만 처리를 할 수 있다. 즉, 암호화부(22)는 고정 폭의 데이터 패킷만을 암호화할 수 있다. 따라서, 임의의 인터페이스 모듈로부터 입력되는, 여러 가지 데이터 폭의 데이터 패킷을 암호화할 수 있기 위해서는, 가변 폭의 데이터 패킷을 고정 폭의 데이터 패킷으로 변환해주는 가변 폭-고정 폭 데이터 패킷 변환부(21)가 암호화부(22) 이전 단에 들어가야 한다.

<37> 암호화부(22)에서 암호화가 완료된 경우, 가변 폭-고정 폭 데이터 패킷 변환부(31)는 암호화부(22)에서 출력된 고정 폭의 암호화 데이터 패킷을 결합 값의 개수로 분리하여, 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 생성하고, 생성된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 출력한다. 상기된 예에서, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 암호화된 32 비트의 데이터 패킷을 결합 값의 개수, 즉 2 개로 분리하여야 한다. 왜냐하면, 외부 인터페이스 모듈에 연결된 입출력 포트 수가 16 비트이기 때문에, 16 비트 데이터 패킷만을 이 입출력 포트를 경유하여 외부 인터페이스 모듈로 내보낼 수 있기 때문이다.

<38> 만약, 가변 폭이 고정 폭의 배수인 경우, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 가변 폭의 데이터 패킷을 입력받고, 입력된 가변 폭의 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고

정 폭의 데이터 패킷을 생성하여 차례로 출력한다. 예를 들어, 가변 폭이 32 비트이고, 고정 폭이 16 비트인 경우, 상기된 가변 폭이 32비트이고, 고정 폭이 16 비트인 경우와는 달리, 외부 인터페이스 모듈로부터 입력된 32 비트의 데이터 패킷을 분리해야 한다. 가변 폭-고정 폭 데이터 패킷 변환부(21)는 이 32 비트의 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수, 즉 2 개로 분리하여, 암호화부(22)에 차례로 출력하면 된다.

<39> 암호화부(22)에서 암호화가 완료된 경우, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 암호화부(22)에서 출력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 차례로 입력받고, 차례로 입력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 결합하여, 가변 폭의 암호화 데이터 패킷을 생성하여 출력한다. 상기된 예에서, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 암호화된 16 비트의 데이터 패킷을 차례로 입력받고, 차례로 입력된 2 개의 16 비트 암호화 데이터 패킷을 결합하여, 32 비트 암호화 데이터 패킷을 생성하고, 생성된 32 비트 암호화 데이터 패킷은 외부 인터페이스 모듈로 출력되게 된다.

<40> 도 3은 상기 도 2의 암호화부(22)의 상세 구성도이다.

<41> 상기 도 2의 암호화부(22)는 고정 폭 데이터 패킷 저장부(31), 고정 폭-암호화 폭 데이터 변환부(32), 암호화 폭 데이터 암호화부(33), 암호화 폭-고정 폭 암호화 데이터 패킷 변환부(34), 고정 폭 암호화 데이터 패킷 저장부(35), 및 암호화 제어부(36)로 구성된다.

<42> 고정 폭 데이터 패킷 저장부(31)는 상기 도 2의 가변 폭-고정 폭 데이터 패킷 변환부(21)에서 생성된 고정 폭의 데이터 패킷을 저장한다. IPSEC 표준안에 따르면, ESP(Encapsulating Security Payload) 메모리 및 AH(Authentication Header) 메모리에 데이터 패킷을 저장한 후, ESP 엔진 및 AH 엔진을 구동시키는 방식을 취하고 있다. 고정 폭 데이터 패킷 저장부(31)는 ESP 메모리 및 AH 메모리의 역할을 담당한다.

<43> 고정 폭-암호화 폭 데이터 변환부(32)는 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환한다. DES(Data Encryption Standard)-CBC(Cipher Block Chaining) 알고리즘을 사용하는 ESP 엔진의 경우, 64 비트인 데이터를 입력받아, 암호화하여, 64 비트인 암호화 데이터를 출력한다. 여기에서, DES-CBC는 보안을 위한 비밀 키 알고리즘이다. IPv6 데이터 패킷의 경우, 데이터량이 최대 1500 바이트까지 가능하기 때문에, 고정 폭-암호화 폭 데이터 변환부(32)는 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷을 잘라서, 64 비트인 데이터를 만들어, DES-CBC 알고리즘을 사용하는 ESP 엔진으로 보내게 된다. 이때, ESP 엔진은 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷 중, 페이로드 필드에 저장된 사용자 데이터만을 암호화한다.

<44> HMAC(Hash Message Authentication Code)-MD5(Message Digest function 95) 알고리즘을 사용하는 AH 엔진의 경우, 32 비트인 데이터를 입력받아, 암호화하여, 32 비트인 암호화 데이터를 출력한다. 여기에서, HMAC-MD5는 인증을 제공하는 비밀 키 알고리즘이다. 고정 폭-암호화 폭 데이터 변환부(32)는 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷을 잘라서, 32 비트인 데이터를 만들어, HMAC MD5 알고리즘을 사용하는 AH 엔진으로 보내게 된다. 이때, AH 엔진은 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷 전체에 대한 인증을 담당하고 있기 때문에, 고정 폭의 데이터 패킷 전체에 대하여 인증을 제공하는 해시 코드를 생성한다.

<45> 암호화 폭 데이터 암호화부(33)는 고정 폭-암호화 폭 데이터 변환부(32)에서 변환된 암호화 폭의 데이터를 암호화하여, 암호화 폭의 암호화 데이터를 생성한다. IP 환경에서, 암호화 폭 데이터 암호화부(33)는 주로 ESP 엔진이나 AH 엔진이 될 것이다. 여기에서, ESP 엔진은 데이터 패킷의 페이로드 부분을 암호화하고, AH 엔진은 데이터 패킷 전체에 대한 인증 코드를 생

성한다. 암호화 폭 데이터 암호화부(33)는 암호화 폭의 암호화 데이터가 생성된 경우, 암호화 완료 신호를 생성하여 출력한다. 암호화가 완료된 경우, 다른 데이터를 암호화할 준비가 되어 있다는 의미에서, 암호화 완료 신호를 생성하여 출력하게 된다.

<46> 암호화 폭-고정 폭 암호화 데이터 패킷 변환부(34)는 암호화 폭 데이터 암호화부(33)에서 생성된 암호화 폭의 암호화 데이터를 고정 폭의 암호화 데이터 패킷으로 변환한다. 암호화 폭 데이터 암호화부(33)가 DES-CBC 알고리즘을 사용하는 ESP 엔진인 경우, 암호화 폭-고정 폭 암호화 데이터 패킷 변환부(34)는 64 비트의 암호화 데이터를 결합하여, 고정 폭의 암호화 데이터 패킷을 만든다. 암호화 폭 데이터 암호화부(33)가 HMAC-MD5 알고리즘을 사용하는 AH 엔진인 경우, 암호화 폭-고정 폭 암호화 데이터 패킷 변환부(34)는 32 비트의 인증 코드를 결합하여, 128 비트 해시 코드가 부착된, 고정 폭의 암호화 데이터 패킷을 만든다.

<47> 고정 폭 암호화 데이터 패킷 저장부(35)는 암호화 폭-고정 폭 암호화 데이터 패킷 변환부(34)에서 변환된 고정 폭의 암호화 데이터 패킷을 저장한다. 고정 폭 암호화 데이터 패킷 저장부(35)는 고정 폭의 암호화 데이터 패킷을 일시적으로 저장하고 있다가, 상기 도 2의 가변 폭-고정 폭 데이터 패킷 변환부(21)로 보내는 역할을 담당한다.

<48> 암호화 제어부(36)는 암호화 폭 데이터 암호화부(33)로부터 출력된 암호화 완료 신호를 입력받은 경우, 고정 폭-암호화 폭 변환 신호를 생성하여 출력한다. 즉, 암호화 과정이 종료된 암호화 폭 데이터 암호화부(33)에 암호화할 데이터를 입력하라는 의미에서, 고정 폭-암호화 폭 데이터 변환부(32)에 고정 폭-암호화 폭 변환 신호를 주게 된다. 이때, 고정 폭-암호화 폭 데이터 변환부(32)는 암호화 제어부(36)로부터 출력된 고정 폭-암호화 폭 변환 신호를 입력받은 경우, 고정 폭 데이터 패킷 저장부(31)에 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환한다.

<49> 도 4는 본 발명의 일 실시예에 따른 가변 폭 암호화 데이터 패킷 복호화 장치의 구성도이다.

<50> 가변 폭 암호화 데이터 패킷 복호화 장치는 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41) 및 복호화부(42)로 구성된다.

<51> 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)는 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우, 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고, 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 고정 폭의 암호화 데이터 패킷을 생성하여 출력한다. 예를 들어, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷(외부로부터 들어온 암호화 데이터 패킷)의 폭이 16 비트이고, 가변 폭 암호화 데이터 패킷 복호화 장치의 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭이 32 비트인 경우, 즉, 가변 폭이 16 비트이고, 고정 폭이 32 비트인 경우, 가변 폭 암호화 데이터 패킷 복호화 장치는 데이터 폭이 32 비트인 데이터 패킷만을 처리할 수 있기 때문에, 외부로부터 입력된 16 비트 암호화 데이터 패킷을 복호화할 수 없다. 따라서, 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)는 두 개의 16 비트 암호화 데이터 패킷들을 차례로 입력받고, 입력받은 두 개의 16 비트 암호화 데이터 패킷들을 결합하여, 32 비트 암호화 데이터 패킷을 만들고, 이 32 비트 암호화 데이터 패킷을 복호화한다.

<52> 복호화부(42)는 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)에서 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 고정 폭의 데이터 패킷을 생성하여 출력한다.

<53> 복호화부(42)에서 복호화가 완료된 경우, 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)는 복호화부(42)에서 출력된 고정 폭의 데이터 패킷을 결합 값의 개수로 분리하여, 결합

값의 개수의 가변 폭의 데이터 패킷을 생성하고, 생성된 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 출력한다. 상기된 예에서, 가변 폭-고정 폭 데이터 패킷 변환부(21)는 복호화된 32 비트의 데이터 패킷을 결합 값의 개수, 즉 2 개로 분리하여야 한다. 왜냐하면, 외부 인터페이스 모듈에 연결된 입출력 포트 수가 16 비트이기 때문에, 16 비트 데이터 패킷만을 이 입출력 포트를 경유하여 외부 인터페이스 모듈로 내보낼 수 있기 때문이다.

<54> 만약, 가변 폭이 상기 고정 폭의 배수인 경우라면, 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)는 가변 폭의 암호화 데이터 패킷을 입력받고, 입력된 가변 폭의 암호화 데이터 패킷을, 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 차례로 출력한다. 예를 들어, 가변 폭이 32 비트이고, 고정 폭이 16 비트인 경우, 상기된 가변 폭이 32비트이고, 고정 폭이 16 비트인 경우와는 달리, 외부 인터페이스 모듈로부터 입력된 32 비트의 암호화 데이터 패킷을 분리해야 한다. 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)는 이 32 비트의 암호화 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수, 즉 2 개로 분리하여, 복호화부(42)에 차례로 출력하면 된다. 데이터 패킷을 분리해야 한다. 가변 폭-고정 폭 암호화 데이터 패킷 변환부(21)는 이 32 비트의 암호화 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수, 즉 2 개로 분리하여, 복호화부(42)에 차례로 출력하면 된다.

<55> 복호화부(42)에서 복호화가 완료된 경우, 가변 폭-고정 폭 암호화 데이터 패킷 변환부는 복호화부(42)에서 출력된 분리 값의 개수의 고정 폭의 데이터 패킷을 차례로 입력받고, 차례로 입력된 분리 값의 개수의 고정 폭의 데이터 패킷을 결합하여, 가변 폭의 데이터 패킷을 생성하여 출력한다. 상기된 예에서, 가변 폭-고정 폭 암호화 데이터 패킷 변환부(21)는 복호화된 16 비트의 데이터 패킷을 차례로 입력받고, 차례로 입력된 2 개의 16 비트 데이터 패킷을 결

합하여, 32 비트 데이터 패킷을 생성하고, 생성된 32 비트 데이터 패킷은 외부 인터페이스 모듈로 출력되게 된다.

<56> 도 5는 상기 도 4의 복호화부(42)의 상세 구성도이다.

<57> 상기 도 4의 복호화부(42)는 고정 폭 암호화 데이터 패킷 저장부(51), 고정 폭-복호화 폭 암호화 데이터 변환부(52), 복호화 폭 암호화 데이터 복호화부(53), 복호화 폭-고정 폭 데이터 패킷 변환부(54), 고정 폭 데이터 패킷 저장부(55), 및 복호화 제어부(56)로 구성된다.

<58> 고정 폭 암호화 데이터 패킷 저장부(51)는 상기 도 4의 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)에서 생성된 고정 폭의 암호화 데이터 패킷을 저장한다. IPSEC 표준안에 따르면, ESP 메모리 및 AH 메모리에 암호화 데이터 패킷을 저장한 후, ESP 엔진 및 AH 엔진을 구동시키는 방식을 취하고 있다. 고정 폭 암호화 데이터 패킷 저장부(51)는 ESP 메모리 및 AH 메모리의 역할을 담당한다.

<59> 고정 폭-복호화 폭 암호화 데이터 변환부(52)는 고정 폭 암호화 데이터 패킷 저장부(51)에 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환한다. DES-CBC 알고리즘을 사용하는 ESP 엔진의 경우, 64 비트인 암호화 데이터를 입력받아, 복호화하여, 64 비트인 데이터를 출력한다. 고정 폭-복호화 폭 암호화 데이터 변환부(52)는 고정 폭 암호화 데이터 패킷 저장부(51)에 저장된 고정 폭의 데이터 패킷을 잘라서, 64 비트인 데이터를 만들어, DES-CBC 알고리즘을 사용하는 ESP 엔진으로 보내게 된다. 이때, ESP 엔진은 고정 폭 암호화 데이터 패킷 저장부(31)에 저장된 고정 폭의 암호화 데이터 패킷 중, 페이로드 필드에 저장된 사용자 데이터만을 복호화한다. HMAC-MD5 알고리즘을 사용하는 AH 엔진의 경우, 32 비트인 암호화 데이터를 입력받아, 복호화하여, 32 비트인 데이터를 출력한다. 고정 폭-복호화 폭 암호화 데이터 변환부(52)는 고정 폭 암호화 데이터 패킷 저장부(51)에 저장된 고정 폭의 암호화 데이

터 패킷을 잘라서, 32 비트인 데이터를 만들어, HMAC MD5 알고리즘을 사용하는 AH 엔진으로 보내게 된다. 이때, AH 엔진은 고정 폭 암호화 데이터 패킷 저장부(51)에 저장된 고정 폭의 데이터 패킷 전체에 대한 인증을 담당하고 있기 때문에, 고정 폭의 암호화 데이터 패킷 전체에 대한 인증 여부를 결정하게 된다.

<60> 복호화 폭 암호화 데이터 복호화부(53)는 고정 폭-복호화 폭 데이터 변환부(52)에서 변환된 복호화 폭의 암호화 데이터를 복호화하여, 복호화 폭의 데이터를 생성한다. IP 환경에서, 복호화 폭 암호화 데이터 복호화부(53)는 주로 ESP 엔진이나 AH 엔진이 될 것이다. 여기에서, ESP 엔진은 데이터 패킷의 페이로드 부분을 복호화하고, AH 엔진은 데이터 패킷 전체에 대한 인증 여부를 결정한다. 복호화 폭 암호화 데이터 복호화부(53)는 복호화 폭의 데이터가 생성된 경우, 복호화 완료 신호를 생성하여 출력한다. 복호화가 완료된 경우, 다른 데이터를 복호화할 준비가 되어 있다는 의미에서, 복호화 완료 신호를 생성하여 출력하게 된다.

<61> 복호화 폭-고정 폭 데이터 패킷 변환부(54)는 복호화 폭 데이터 복호화부(53)에서 생성된 복호화 폭의 데이터를 고정 폭의 데이터 패킷으로 변환한다. 복호화 폭 데이터 복호화부(53)가 DES-CBC 알고리즘을 사용하는 ESP 엔진인 경우, 복호화 폭-고정 폭 데이터 패킷 변환부(54)는 64 비트의 데이터를 결합하여, 고정 폭의 데이터 패킷을 만든다. 복호화 폭 데이터 복호화부(53)가 HMAC-MD5 알고리즘을 사용하는 AH 엔진인 경우, 복호화 폭-고정 폭 데이터 패킷 변환부(54)는 32 비트의 인증 코드를 결합하여, 128 비트의 인증 코드를 만들어, 인증 여부를 결정하게 된다.

<62> 고정 폭 데이터 패킷 저장부(55)는 복호화 폭-고정 폭 데이터 패킷 변환부(54)에서 변환된 고정 폭의 데이터 패킷을 저장한다. 고정 폭 데이터 패킷 저장부(55)는 고정 폭의 데이터

패킷을 일시적으로 저장하고 있다가, 상기 도 4의 가변 폭-고정 폭 암호화 데이터 패킷 변환부(41)로 보내는 역할을 담당한다.

<63> 복호화 제어부(56)는 복호화 폭 암호화 데이터 복호화부(53)로부터 출력된 복호화 완료 신호를 입력받은 경우, 고정 폭-복호화 폭 변환 신호를 생성하여 출력한다. 즉, 복호화 과정이 종료된 복호화 폭 암호화 데이터 복호화부(53)에 복호화할 데이터를 입력하라는 의미에서, 고정 폭-복호화 폭 암호화 데이터 변환부(52)에 고정 폭-복호화 폭 변환 신호를 주게 된다. 이때, 고정 폭-복호화 폭 암호화 데이터 변환부(52)는 복호화 제어부(56)로부터 출력된 고정 폭-복호화 폭 변환 신호를 입력받은 경우, 고정 폭 암호화 데이터 패킷 저장부(51)에 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환한다.

<64> 도 6은 본 발명을 적용한 IPSEC 암/복호화 장치의 일 예를 보여주는 도면이다.

<65> 본 발명을 적용한 IPSEC 암/복호화 장치는 가변 폭-고정 폭 (암호화) 데이터 패킷 변환부(61), 고정 폭 (암호화) 데이터 패킷 저장부(62, 68), 고정 폭-복호화 폭 암/복호화 (암호화) 데이터 변환부(63, 69), 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610), 암/복호화 폭-고정 폭 (암호화) 데이터 패킷 변환부(65, 611), 고정 폭 (암호화) 데이터 패킷 저장부(66), 및 암/복호화 제어부(67)로 구성된다.

<66> 상기 도 6을 보면, 가변 폭-고정 폭 (암호화) 데이터 패킷 변환부(61)는 이부 인터페이스 모듈로부터 가변 N 비트의 데이터 패킷이나, 가변 N 비트의 암호화 데이터 패킷을 입력받아, 고정 m 비트의 데이터 패킷을 변환하여, 고정 폭 (암호화) 데이터 패킷 저장부(62, 68)에 저장한다. 이것들은 각각 ESP 메모리와 AH 메모리에 해당한다. 고정 폭-복호화 폭 암/복호화 (암호화) 데이터 변환부(63, 69)는 저장된 데이터 패킷 또는 암호화 데이터 패킷을 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610), 즉 ESP 엔진과 AH 엔진에서 처리 가능한 용량

인 k1 비트 데이터와 k2 비트 데이터로 변환한다. 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610), 즉 ESP 엔진과 AH 엔진은 각각 k1 비트 데이터와 k2 비트 데이터를 암호화하거나, k1 비트 암호화 데이터와 k2 암호화 비트 데이터를 복호화한다. 암/복호화 폭-고정 폭 (암호화) 데이터 패킷 변환부(65, 611)는 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610)에서 암호화 또는 복호화된 데이터를 m 비트 암호화 데이터 패킷 또는 m 비트 데이터 패킷으로 변환한다. 상기의 과정을 거쳐, m 비트 암호화 데이터 패킷 또는 m 비트 데이터 패킷이 생성되면, 고정 폭 (암호화) 데이터 패킷 저장부(66)에 저장되게 된다. 고정 폭 (암호화) 데이터 패킷 저장부(66)에 저장된 m 비트 암호화 데이터 패킷 또는 m 비트 데이터 패킷은 가변 N 비트 암호화 데이터 패킷 또는 가변 N 비트 데이터 패킷으로 변환되어, 외부 인터페이스 모듈로 출력되게 된다. 암/복호화 제어부(67)는 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610), 즉 ESP 엔진과 AH 엔진에서 암호화 또는 복호화가 완료된 경우, 고정 폭-복호화 폭 암/복호화 (암호화) 데이터 변환부(63, 69)로부터 암/복호화 폭 (암호화) 데이터 암/복호화부(64, 610)로 바로 암호화 또는 복호화하고자 하는 데이터가 입력될 수 있도록, 고정 폭-복호화 폭 암/복호화 (암호화) 데이터 변환부(63, 69)를 제어한다.

<67> 도 7은 본 발명의 일 실시예에 따른 가변 폭-고정 폭 데이터 패킷 변환 장치의 구성도이다.

<68> 가변 폭-고정 폭 데이터 패킷 변환 장치는 가변 폭 데이터 패킷 입출력부(71), 가변 폭 데이터 패킷 결합부(72), 고정 폭 데이터 패킷 분리부(73), 가변 폭 데이터 패킷 분리부(74), 고정 폭 데이터 패킷 결합부(75), 고정 폭 데이터 패킷 입출력부(76)로 구성된다.

<69> 가변 폭 데이터 패킷 입출력부(71)는 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 고정 폭을

가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는다. 상기된 가변 폭 데이터 패킷 암/복호화 장치에 사용되는 가변 폭-고정 폭 데이터 패킷 변환 장치는 암/복호화 장치뿐만 아니라, 여러 장치들에 사용될 수 있다. IPv6 환경에서는 IPv4 환경과는 달리, 특성상 다양한 플랫폼(예를 들면, 가정내의 모든 가전기기)에서 구동되어야 할 것이므로, 외부 인터페이스 모듈의 변경이 빈번하게 발생할 것이다. 따라서, 외부 인터페이스 모듈을 필요로 하는, 모든 주변 장치들에 가변 폭-고정 폭 데이터 패킷 변환 장치가 사용되어야 할 것이다. 가변 폭 데이터 패킷 입출력부(71)는 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 고정 폭의 제 1 데이터 패킷 하나를 만들기 위하여, 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는다.

<70> 가변 폭 데이터 패킷 결합부(72)는 가변 폭 데이터 패킷 입출력부(71)에 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 고정 폭의 제 1 데이터 패킷을 생성한다. 고정 폭 데이터 패킷 입출력부(76)는 가변 폭 데이터 패킷 결합부(72)에서 생성된 고정 폭의 제 1 데이터 패킷을 출력한다.

<71> 고정 폭 데이터 패킷 입출력부(76)에서 출력된 고정 폭의 제 1 데이터는 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈, 예를 들면 암호화 모듈, 복호화 모듈에 입력되고, 다시 이 모듈로부터 고정 폭의 제 2 데이터가 출력된다. 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈이 암호화 모듈인 경우라면, 제 2 데이터 패킷은 제 1 데이터 패킷으로부터 암호화된 데이터 패킷일 것이고, 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈이 복호화 모듈인 경우라면, 제 2 데이터 패킷은 제 1 데이터 패킷으로부터 복호화된 데이터 패킷인 것이다.

<72> 고정 폭 데이터 패킷 입출력부(76)는 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈로부터 고정 폭의 제 2 데이터 패킷을 입력받는다. 고정 폭 데이터 패킷 분리부(73)는 고정 폭 데이터 패킷 입출력부(76)에 입력된 고정 폭의 제 2 데이터 패킷을 결합 값의 개수로 분리하여, 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 생성한다. 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈 내에서 처리하기 위하여, 고정 폭의 데이터 패킷으로 변환하였고, 처리가 완료된 경우, 다시 외부에서 처리될 수 있는, 가변 폭의 데이터 패킷으로 변환하기 위하여, 고정 폭의 데이터 패킷을 결합 값의 개수로 분리한다. 가변 폭 데이터 패킷 입출력부(71)는 고정 폭 데이터 패킷 분리부(73)에서 생성된 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 출력한다.

<73> 가변 폭 데이터 패킷 입출력부(71)는 가변 폭이 고정 폭의 배수인 경우, 가변 폭의 제 1 데이터 패킷 하나를 입력받는다. 가변 폭 데이터 패킷 분리부(74)는 가변 폭 데이터 패킷 입출력부(71)에 입력된 가변 폭의 제 1 데이터 패킷을 가변 폭을 고정 폭로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 생성한다. 가변 폭 데이터 패킷 분리부(74)는 가변 폭의 제 1 데이터 패킷 하나를 가변 폭을 고정 폭로 나눈 값인 분리 값의 개수로 분리하여, 암호화 모듈 또는 복호화 모듈에서 처리할 수 있는 고정 폭의 제 1 데이터 패킷으로 만든다. 고정 폭 데이터 패킷 입출력부(76)는 가변 폭 데이터 패킷 분리부(74)에서 생성된 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 차례로 출력한다. 일반적으로, 암호화 모듈 또는 복호화 모듈은 패킷 단위로 데이터를 처리하기 때문에, 암호화 모듈 또는 복호화 모듈이 한 패킷을 처리한 즉시, 가변 폭-고정 폭 데이터 패킷 변환 장치는 암호화 모듈 또는 복호화 모듈에 다른 패킷을 입력하여야 한다. 종래에는 패킷 프로세서가 별도로 존재하여

, 패킷의 흐름을 조절하는 역할을 하였으나, 본 발명에서는, 가변 폭-고정 폭 데이터 패킷 변환 장치가 패킷 프로세서의 역할도 병행하고 있다.

<74> 상기한 바와 같이, 고정 폭 데이터 패킷 입출력부(76)에서 출력된 고정 폭의 제 1 데이터는 가변 폭-고정 폭 데이터 패킷 변환 장치가 탑재된 모듈, 예를 들면 암호화 모듈, 복호화 모듈에 입력되고, 다시 이 모듈로부터 고정 폭의 제 2 데이터가 출력된다. 고정 폭 데이터 패킷 입출력부(76)는 가변 폭이 고정 폭의 배수인 경우, 가변 폭을 고정 폭으로 나눈 값인, 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력받는다. 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭이, 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭의 배수인 경우이므로, 가변 폭의 제 2 데이터 패킷 하나를 만들기 위하여, 고정 폭 데이터 패킷 입출력부(76)는 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력받는다.

<75> 고정 폭 데이터 패킷 결합부(75)는 고정 폭 데이터 패킷 입출력부(76)에 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합하여, 가변 폭의 제 2 데이터 패킷을 생성한다. 가변 폭 데이터 패킷 입출력부(71)는 고정 폭 데이터 패킷 결합부(75)에서 생성된 가변 폭의 제 2 데이터 패킷을 출력한다.

<76> 도 8은 상기 도 7의 가변 폭 데이터 패킷 결합부의 상세 구성도이다.

<77> 가변 폭 데이터 패킷 결합부는 가변 폭 데이터 패킷 저장부(81), 저장 가변 폭 데이터 패킷 결합부(82), 및 결합 값 카운트부(83)로 구성된다.

<78> 가변 폭 데이터 패킷 저장부(81)는 가변 폭 데이터 패킷 입출력부에 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 저장한다. 고정 폭이 가변 폭의 배수인 경우, 예를 들면, 고정 폭이 32 비트이고, 가변 폭이 16 비트인 경우, 고정 폭의 제 1 데이터 패

킷을 만들려면, 가변 폭의 데이터 패킷 2 개를 결합하여야 하는데, 이를 위해서 실시간으로 입력되는 가변 폭의 데이터 패킷 2 개를 저장해 놓아야 한다. 이 때, 일반적으로 저용량 저장 장치인 레지스터를 사용하는데, 레지스터는 전체 읽기/쓰기만 가능하기 때문에, 32 비트 레지스터 하나, 16 비트 레지스터 하나, 8 비트 레지스터 2 개, 4 비트 레지스터 4 개, 2 비트 레지스터 8 개, 1 비트 레지스터 16 개 등 전체 32 개의 레지스터를 사용하여야 한다. 16 비트 제 1 데이터 패킷 2 개는 각각 입력된 순서에 따라, 먼저 32 비트 레지스터에 저장되고, 이어서 16 비트 레지스터에 저장된다. 만약, 가변 폭이 1 비트인 경우라면, 1 비트 제 1 데이터 패킷 32 개가 전체 32 개의 레지스터에 차례대로 저장된다.

<79> 저장 가변 폭 데이터 패킷 결합부(82)는 가변 폭 데이터 패킷 저장부(82)에 차례로 저장된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 고정 폭의 제 1 데이터 패킷을 생성한다. 결합 값 카운트부(83)는 결합 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 생성된 결합 신호를 출력한다. 이때, 저장 가변 폭 데이터 패킷 결합부(82)는 결합 값 카운트부(83)에서 출력된 결합 신호를 입력받을 때마다, 저장된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 결합한다. 예를 들면, 고정 폭이 32 비트이고, 가변 폭이 16 비트인 경우, 결합 값은 2가 될 것이고, 결합 값 카운트부(83)는 1을 카운트한다. 따라서, 카운트 횟수는 한 번이 될 것이고, 결합 신호는 한 번 출력된다. 저장 가변 폭 데이터 패킷 결합부(82)는 결합 신호를 한 번 입력받고, 이때 저장된 16 비트 제 1 데이터 패킷을 결합하여, 32 비트 제 1 데이터 패킷을 만든다.

<80> 도 9는 상기 도 7의 고정 폭 데이터 패킷 결합부의 상세 구성도이다.

<81> 고정 폭 데이터 패킷 결합부는 고정 폭 데이터 패킷 저장부(91), 저장 고정 폭 데이터 패킷 결합부(92), 및 분리 값 카운트부(93)로 구성된다.

<82> 고정 폭 데이터 패킷 저장부(91)는 고정 폭 데이터 패킷 입출력부에 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 저장한다. 고정 폭이 가변 폭의 배수인 경우, 예를 들면, 가변 폭이 32 비트이고, 고정 폭이 16 비트인 경우, 가변 폭의 제 2 데이터 패킷을 만들려면, 고정 폭의 데이터 패킷 2 개를 결합하여야 하는데, 이를 위해서 실시간으로 입력되는 가변 폭의 데이터 패킷 2 개를 저장해 놓아야 한다. 레지스터는 전체 읽기/쓰기만 가능하기 때문에, 16 비트 레지스터 2 개를 사용하여야 한다. 16 비트 제 1 데이터 패킷 2 개는 각각 입력된 순서에 따라, 16 비트 레지스터 2 개에 차례로 저장된다. 만약, 가변 폭이 64 비트인 경우라면, 16 비트 레지스터는 4 개가 필요하다. 따라서, 임의의 외부 인터페이스 모듈에 대응하기 위해서는 충분한 개수의 고정 폭의 레지스터를 구비하고 있어야 한다.

<83> 저장 고정 폭 데이터 패킷 결합부(92)는 고정 폭 데이터 패킷 저장부(91)에 차례로 저장된 고정 폭의 제 2 데이터 패킷을 결합하여, 가변 폭의 제 2 데이터 패킷을 생성한다. 분리 값 카운트부(93)는 분리 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 생성된 결합 신호를 출력한다. 이때, 저장 고정 폭 데이터 패킷 결합부(92)는 분리 값 카운트부(93)에서 출력된 결합 신호를 입력받을 때마다, 저장된 분리 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 결합한다. 예를 들면, 가변 폭이 32 비트이고, 고정 폭이 16 비트인 경우, 분리 값은 2가 될 것이고, 분리 값 카운트부(93)는 1을 카운트한다. 따라서, 카운트 횟수는 한 번이 될 것이고, 분리 신호는 한 번 출력된다. 저장 고정 폭 데이터 패킷 결합부(91)는 분리 신호를 한 번 입력받고, 이때 저장된 16 비트 제 2 데이터 패킷을 결합하여, 32 비트 제 2 데이터 패킷을 만든다.

<84> 도 10은 본 발명의 일 실시예에 따른 가변 폭 데이터 패킷 암호화 방법의 흐름도이다.

<85> 만약, 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우라면(101), 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고(102), 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 고정 폭의 데이터 패킷을 생성하여 출력한다(103). 이어서, 출력된 고정 폭의 데이터 패킷을 암호화하여, 고정 폭의 암호화 데이터 패킷을 생성하여 출력한다(104). 이어서, 출력된 고정 폭의 암호화 데이터 패킷을 결합 값의 개수로 분리하여, 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 생성하고(105), 생성된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 출력한다(106).

<86> 만약, 가변 폭이 고정 폭의 배수인 경우라면(101), 가변 폭의 데이터 패킷을 입력받고(107), 입력된 가변 폭의 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 차례로 출력한다(108). 이어서, 출력된 분리 값의 개수의 고정 폭의 데이터 패킷을 암호화하여, 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 출력한다(109). 이어서, 출력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 차례로 입력받고, 차례로 입력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 결합하여(1010), 가변 폭의 암호화 데이터 패킷을 생성하여 출력한다(1011).

<87> 도 11은 상기 도 10의 104 단계, 109 단계의 상세 흐름도이다.

<88> 생성된 고정 폭의 데이터 패킷을 저장한다(111). 이어서, 출력된 고정 폭-암호화 폭 변환 신호를 입력받은 경우(112), 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환한다(113). 이어서, 변환된 암호화 폭의 데이터를 암호화하여, 암호화 폭의 암호화 데이터를 생성하고, 암호화 폭의 암호화 데이터가 생성된 경우, 암호화 완료 신호를 생성하여 출력한다(114). 이어서, 출력된 암호화 완료 신호를 입력받은 경우(115), 고정 폭-암호화 폭 변환 신호

를 생성하여 출력한다(116). 이어서, 생성된 암호화 폭의 암호화 데이터를 고정 폭의 암호화 데이터 패킷으로 변환한다(117). 이어서, 변환된 고정 폭의 암호화 데이터 패킷을 저장한다(118).

<89> 도 12는 본 발명의 일 실시예에 따른 가변 폭 암호화 데이터 패킷 복호화 방법의 흐름도이다.

<90> 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우(121), 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고(122), 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 고정 폭의 암호화 데이터 패킷을 생성하여 출력한다(123). 이어서, 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 고정 폭의 데이터 패킷을 생성하여 출력한다(124). 이어서, 출력된 고정 폭의 데이터 패킷을 결합 값의 개수로 분리하여, 결합 값의 개수의 가변 폭의 데이터 패킷을 생성하고(125), 생성된 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 출력한다(126).

<91> 만약, 가변 폭이 고정 폭의 배수인 경우라면(121), 가변 폭의 암호화 데이터 패킷을 입력받고(127), 입력된 가변 폭의 암호화 데이터 패킷을 가변 폭을 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 차례로 출력한다(128). 이어서, 출력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 복호화하여, 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 출력한다(129). 이어서, 출력된 분리 값의 개수의 고정 폭의 데이터 패킷을 차례로 입력받고, 차례로 입력된 분리 값의 개수의 고정 폭의 데이터 패킷을 결합하여(1210), 가변 폭의 데이터 패킷을 생성하여 출력한다(1211).

<92> 도 13은 상기 도 12의 124 단계, 129 단계의 상세 흐름도이다.

<93> 생성된 고정 폭의 암호화 데이터 패킷을 저장한다(131). 이어서, 출력된 고정 폭-복호화 폭 변환 신호를 입력받은 경우(132), 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환한다(133). 이어서, 변환된 복호화 폭의 암호화 데이터를 복호화하여, 복호화 폭의 데이터를 생성하고, 복호화 폭의 데이터가 생성된 경우, 복호화 완료 신호를 생성하여 출력한다(134). 이어서, 출력된 복호화 완료 신호를 입력받은 경우(135), 고정 폭-복호화 폭 변환 신호를 생성하여 출력한다(136). 이어서, 생성된 복호화 폭의 데이터를 고정 폭의 데이터 패킷으로 변환한다(137). 이어서, 변환된 고정 폭의 데이터 패킷을 저장한다(138).

<94> 도 14는 본 발명의 일 실시예에 다른 가변 폭-고정 폭 데이터 패킷 변환 방법의 흐름도이다.

<95> 만약, 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우라면(141), 고정 폭을 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는다(142). 이어서, 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 고정 폭의 제 1 데이터 패킷을 생성한다(143). 이어서, 생성된 고정 폭의 제 1 데이터 패킷을 암/복호화 모듈에 출력한다(144). 이어서, 이 암/복호화 모듈로부터 고정 폭의 제 2 데이터 패킷을 입력받는다(145). 이어서, 입력된 고정 폭의 제 2 데이터 패킷을 결합 값의 개수로 분리하여, 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 생성한다(146). 이어서, 생성된 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 출력한다(147).

<96> 만약, 가변 폭이 고정 폭의 배수인 경우라면(141), 가변 폭의 제 1 데이터 패킷을 입력받는다(148). 이어서, 입력된 가변 폭의 제 1 데이터 패킷을 가변 폭을 고정 폭로 나눈 값인 분리 값의 개수로 분리하여, 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 생성한다(149).

이어서, 생성된 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 암/복호화 모듈에 차례로 출력한다(1410). 이어서, 이 암/복호화 모듈로부터 가변 폭을 고정 폭으로 나눈 값인, 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력받는다(1411). 이어서, 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합하여, 가변 폭의 제 2 데이터 패킷을 생성한다(1412). 이어서, 생성된 가변 폭의 제 2 데이터 패킷을 출력한다(1413).

<97> 여기에서, 암/복호화 모듈이 암호화 모듈인 경우라면, 제 2 데이터 패킷은 제 1 데이터 패킷으로부터 암호화된 데이터 패킷이 될 것이고, 암/복호화 모듈이 복호화 모듈인 경우라면, 제 2 데이터 패킷은 제 1 데이터 패킷으로부터 복호화된 데이터 패킷이 될 것이다.

<98> 도 15는 상기 도 14의 143 단계의 상세 흐름도이다.

<99> 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 저장한다(151). 이어서, 결합 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 상기 생성된 결합 신호를 출력한다(152). 이어서, 출력된 결합 신호를 입력받을 때마다(153), 차례로 저장된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 고정 폭의 제 1 데이터 패킷을 생성한다(154).

<100> 도 16은 상기 도 14의 1412 단계의 상세 흐름도이다.

<101> 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 저장한다(161). 이어서, 분리 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 생성된 결합 신호를 출력한다(162). 이어서, 출력된 결합 신호를 입력받을 때마다(163), 차례로 저장된 결합 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 결합하여, 가변 폭의 제 2 데이터 패킷을 생성한다(164).

<102> 한편, 상술한 본 발명의 실시예들은 컴퓨터에서 실행될 수 있는 프로그램으로 작성가능하고, 컴퓨터로 읽을 수 있는 기록매체를 이용하여 상기 프로그램을 동작시키는 범용 디지털 컴퓨터에서 구현될 수 있다.

<103> 또한 상술한 본 발명의 실시예에서 사용된 데이터 패킷의 구조는 컴퓨터로 읽을 수 있는 기록매체에 여러 수단을 통하여 기록될 수 있다.

<104> 상기 컴퓨터로 읽을 수 있는 기록 매체는 마그네틱 저장매체(예를 들면, 롬, 플로피 디스크, 하드디스크 등), 광학적 판독 매체(예를 들면, 씨디롬, 디브이디 등) 및 캐리어 웨이브(예를 들면, 인터넷을 통한 전송)와 같은 저장매체를 포함한다.

<105> 이제까지 본 발명에 대하여 그 바람직한 실시예들을 중심으로 살펴보았다. 본 발명이 속하는 기술 분야에서 통상의 지식을 가진 자는 본 발명이 본 발명의 본질적인 특성에서 벗어나지 않는 범위에서 변형된 형태로 구현될 수 있음을 이해할 수 있을 것이다. 그러므로, 개시된 실시예들은 한정적인 관점이 아니라 설명적인 관점에서 고려되어야 한다. 본 발명의 범위는 전술한 설명이 아니라 특허청구범위에 나타나 있으며, 그와 동등한 범위 내에 있는 모든 차이점은 본 발명에 포함된 것으로 해석되어야 할 것이다.

【발명의 효과】

<106> 본 발명에 따르면, IPSEC 칩에 연결되는 외부 인터페이스 모듈이 변경된 경우, 임의의 외부 인터페이스 모듈로부터 출력되는 가변 폭의 데이터 패킷을 암호화하고, 가변 폭의 암호화 데이터 패킷을 복호화할 수 있다는 효과가 있다. 특히, IPv6 환경에서는 IPv4 환경과는 달리, 특성상 다양한 플랫폼(예를 들면, 가정내의 모든 가전기기)에서 구동되어야 할 것이므로, 외부 인터페이스 모듈의 변경이 빈번하게 발생할 것이고, 이것으로 말미암아, IPSEC 칩을 변경하여

재설계하는 경우에도, 메모리 컨트롤러 상위 단의 인터페이스 부분만을 재설계하면 되기 때문에, 메모리 컨트롤러를 포함한 IPSEC 코어를 재설계할 필요가 없다는 효과가 있다.

【특허청구범위】

【청구항 1】

암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 가변 폭-고정 폭 데이터 패킷 변환부; 및

상기 가변 폭-고정 폭 데이터 패킷 변환부에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 암호화부를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 2】

제 1 항에 있어서, 상기 가변 폭-고정 폭 데이터 패킷 변환부는 상기 암호화부에서 출력된 고정 폭의 암호화 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 생성하고, 상기 생성된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 출력하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 3】

제 1 항에 있어서,

상기 가변 폭-고정 폭 데이터 패킷 변환부는 상기 가변 폭이 상기 고정 폭의 배수인 경우, 상기 가변 폭의 데이터 패킷을 입력받고, 상기 입력된 가변 폭의 데이터 패킷을 상기 가변

폭을 상기 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 차례로 출력하고,

상기 암호화부는 상기 가변 폭-고정 폭 데이터 패킷 변환부에서 출력된 분리 값의 개수의 고정 폭의 데이터 패킷을 암호화하여, 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 4】

제 3 항에 있어서, 상기 가변 폭-고정 폭 데이터 패킷 변환부는 상기 암호화부에서 출력된 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 결합하여, 상기 가변 폭의 암호화 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 5】

제 1 항에 있어서, 상기 암호화부는

상기 가변 폭-고정 폭 데이터 패킷 변환부에서 생성된 고정 폭의 데이터 패킷을 저장하는 고정 폭 데이터 패킷 저장부;

상기 고정 폭 데이터 패킷 저장부에 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환하는 고정 폭-암호화 폭 데이터 변환부;

상기 고정 폭-암호화 폭 데이터 변환부에서 변환된 암호화 폭의 데이터를 암호화하여, 상기 암호화 폭의 암호화 데이터를 생성하는 암호화 폭 데이터 암호화부;

상기 암호화 폭 데이터 암호화부에서 생성된 암호화 폭의 암호화 데이터를 상기 고정 폭의 암호화 데이터 패킷으로 변환하는 암호화 폭-고정 폭 암호화 데이터 패킷 변환부; 및

상기 암호화 폭-고정 폭 암호화 데이터 패킷 변환부에서 변환된 고정 폭의 암호화 데이터 패킷을 저장하는 고정 폭 암호화 데이터 패킷 저장부를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 6】

제 3 항에 있어서,

상기 암호화 폭 데이터 암호화부는 상기 암호화 폭의 암호화 데이터가 생성된 경우, 암호화 완료 신호를 생성하여 출력하고,

상기 암호화 폭 데이터 암호화부로부터 출력된 암호화 완료 신호를 입력받은 경우, 고정 폭-암호화 폭 변환 신호를 생성하여 출력하는 암호화 제어부를 포함하고,

상기 고정 폭-암호화 폭 데이터 변환부는 상기 암호화 제어부로부터 출력된 고정 폭-암호화 폭 변환 신호를 입력받은 경우, 상기 고정 폭 데이터 패킷 저장부에 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 장치.

【청구항 7】

복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 가변 폭-고정 폭 암호화 데이터 패킷 변환부; 및

상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부에서 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 복호화부를 포함하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 8】

제 7 항에 있어서, 상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부는 상기 복호화부에서 출력된 고정 폭의 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 데이터 패킷을 생성하고, 상기 생성된 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 출력하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 9】

제 7 항에 있어서,

상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부는 상기 가변 폭이 상기 고정 폭의 배수인 경우, 상기 가변 폭의 암호화 데이터 패킷을 입력받고, 상기 입력된 가변 폭의 암호화 데이터 패킷을 상기 가변 폭을 상기 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 차례로 출력하고,

상기 복호화부는 상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부에서 출력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 10】

제 9 항에 있어서, 상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부는 상기 복호화부에서 출력된 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입

력된 분리 값의 개수의 고정 폭의 데이터 패킷을 결합하여, 상기 가변 폭의 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 11】

제 7 항에 있어서, 상기 복호화부는

상기 가변 폭-고정 폭 암호화 데이터 패킷 변환부에서 생성된 고정 폭의 암호화 데이터 패킷을 저장하는 고정 폭 암호화 데이터 패킷 저장부;

상기 고정 폭 암호화 데이터 패킷 저장부에 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환하는 고정 폭-복호화 폭 암호화 데이터 변환부;

상기 고정 폭-복호화 폭 데이터 변환부에서 변환된 복호화 폭의 암호화 데이터를 복호화하여, 상기 복호화 폭의 데이터를 생성하는 복호화 폭 암호화 데이터 복호화부;

상기 복호화 폭 데이터 복호화부에서 생성된 복호화 폭의 데이터를 상기 고정 폭의 데이터 패킷으로 변환하는 복호화 폭-고정 폭 데이터 패킷 변환부; 및

상기 복호화 폭-고정 폭 데이터 패킷 변환부에서 변환된 고정 폭의 데이터 패킷을 저장하는 고정 폭 데이터 패킷 저장부를 포함하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 12】

제 11 항에 있어서,

상기 복호화 폭 암호화 데이터 복호화부는 상기 복호화 폭의 데이터가 생성된 경우, 복호화 완료 신호를 생성하여 출력하고,

상기 복호화 폭 암호화 데이터 복호화부로부터 출력된 복호화 완료 신호를 입력받은 경우, 고정 폭-복호화 폭 변환 신호를 생성하여 출력하는 복호화 제어부를 포함하고,

상기 고정 폭-복호화 폭 암호화 데이터 변환부는 상기 복호화 제어부로부터 출력된 고정 폭-복호화 폭 변환 신호를 입력받은 경우, 상기 고정 폭 암호화 데이터 패킷 저장부에 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 장치.

【청구항 13】

시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는 가변 폭 데이터 패킷 입출력부;

상기 가변 폭 데이터 패킷 입출력부에 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 상기 고정 폭의 제 1 데이터 패킷을 생성하는 가변 폭 데이터 패킷 결합부; 및

상기 가변 폭 데이터 패킷 결합부에서 생성된 고정 폭의 제 1 데이터 패킷을 출력하는 고정 폭 데이터 패킷 입출력부를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 14】

제 13 항에 있어서, 상기 가변 폭 데이터 패킷 결합부는

상기 가변 폭 데이터 패킷 입출력부에 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 저장하는 가변 폭 데이터 패킷 저장부; 및

상기 가변 폭 데이터 패킷 저장부에 차례로 저장된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 제 1 데이터 패킷을 생성하는 저장 가변 폭 데이터 패킷 결합부를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 15】

제 14 항에 있어서, 상기 가변 폭 데이터 패킷 결합부는

상기 결합 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 상기 생성된 결합 신호를 출력하는 결합 값 카운트부를 포함하고,

상기 저장 가변 폭 데이터 패킷 결합부는 상기 결합 값 카운트부에서 출력된 결합 신호를 입력받을 때마다, 상기 저장된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 결합하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 16】

제 13 항에 있어서,

상기 고정 폭 데이터 패킷 입출력부는 상기 고정 폭의 제 2 데이터 패킷을 입력받고,

상기 고정 폭 데이터 패킷 입출력부에 입력된 고정 폭의 제 2 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 생성하는 고정 폭 데이터 패킷 분리부를 포함하고,

상기 가변 폭 데이터 패킷 입출력부는 상기 고정 폭 데이터 패킷 분리부에서 생성된 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 출력하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 17】

제 13 항에 있어서,

상기 가변 폭 데이터 패킷 입출력부는 상기 가변 폭이 상기 고정 폭의 배수인 경우, 가변 폭의 제 1 데이터 패킷을 입력받고,

상기 가변 폭 데이터 패킷 입출력부에 입력된 가변 폭의 제 1 데이터 패킷을 상기 가변 폭을 상기 고정 폭로 나눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 생성하는 가변 폭 데이터 패킷 분리부를 포함하고,

상기 고정 폭 데이터 패킷 입출력부는 상기 가변 폭 데이터 패킷 분리부에서 생성된 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 차례로 출력하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 18】

제 13 항에 있어서,

상기 고정 폭 데이터 패킷 입출력부는 상기 가변 폭을 상기 고정 폭으로 나눈 값인, 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력받고,

상기 고정 폭 데이터 패킷 입출력부에 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합하여, 상기 가변 폭의 제 2 데이터 패킷을 생성하는 고정 폭 데이터 패킷 결합부를 포함하고,

상기 가변 폭 데이터 패킷 입출력부는 상기 고정 폭 데이터 패킷 결합부에서 생성된 가변 폭의 제 2 데이터 패킷을 출력하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 19】

제 18 항에 있어서, 상기 고정 폭 데이터 패킷 결합부는

상기 고정 폭 데이터 패킷 입출력부에 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 저장하는 고정 폭 데이터 패킷 저장부; 및

상기 고정 폭 데이터 패킷 저장부에 차례로 저장된 고정 폭의 제 2 데이터 패킷을 결합하여, 상기 가변 폭의 제 2 데이터 패킷을 생성하는 저장 고정 폭 데이터 패킷 결합부를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 20】

제 19 항에 있어서, 상기 고정 폭 데이터 패킷 결합부는

상기 분리 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 상기 생성된 결합 신호를 출력하는 분리 값 카운트부를 포함하고,

상기 저장 고정 폭 데이터 패킷 결합부는 상기 분리 값 카운트부에서 출력된 결합 신호를 입력받을 때마다, 상기 저장된 분리 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 결합하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 21】

제 16 항 또는 제 20 항에 있어서, 상기 제 2 데이터 패킷은 상기 제 1 데이터 패킷으로부터 암호화된 데이터 패킷인 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 22】

제 16 항 또는 제 20 항에 있어서, 상기 제 2 데이터 패킷은 상기 제 1 데이터 패킷으로부터 복호화된 데이터 패킷인 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 장치.

【청구항 23】

(a) 암호화 과정에서 처리되는 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 단계; 및

(b) 상기 (a) 단계에서 출력된 고정 폭의 데이터 패킷을 암호화하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 24】

제 23 항에 있어서,

(c) 상기 (b) 단계에서 출력된 고정 폭의 암호화 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 생성하고, 상기 생성된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 25】

제 23 항에 있어서,

상기 (a) 단계는 상기 가변 폭이 상기 고정 폭의 배수인 경우, 상기 가변 폭의 데이터 패킷을 입력받고, 상기 입력된 가변 폭의 데이터 패킷을 상기 가변 폭을 상기 고정 폭으로 나

눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 차례로 출력하고,

상기 (b) 단계는 상기 (a) 단계에서 출력된 분리 값의 개수의 고정 폭의 데이터 패킷을 암호화하여, 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 26】

제 25 항에 있어서,

(d) 상기 (a) 단계에서 출력된 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 결합하여, 상기 가변 폭의 암호화 데이터 패킷을 생성하여 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 27】

제 23 항에 있어서, 상기 (b) 단계는

(b1) 상기 (a) 단계에서 생성된 고정 폭의 데이터 패킷을 저장하는 단계;

(b2) 상기 (b1) 단계에서 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환하는 단계;

(b3) 상기 (b2) 단계에서 변환된 암호화 폭의 데이터를 암호화하여, 상기 암호화 폭의 암호화 데이터를 생성하는 단계;

(b4) 상기 (b3) 단계에서 생성된 암호화 폭의 암호화 데이터를 상기 고정 폭의 암호화 데이터 패킷으로 변환하는 단계; 및

(b5) 상기 (b4) 단계에서 변환된 고정 폭의 암호화 데이터 패킷을 저장하는 단계를 포함하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 28】

제 25 항에 있어서,

상기 (b3) 단계는 상기 암호화 폭의 암호화 데이터가 생성된 경우, 암호화 완료 신호를 생성하여 출력하고,

(b6) 상기 (b3) 단계에서 출력된 암호화 완료 신호를 입력받은 경우, 고정 폭-암호화 폭 변환 신호를 생성하여 출력하는 단계를 포함하고,

상기 (b2) 단계는 상기 (b6) 단계로부터 출력된 고정 폭-암호화 폭 변환 신호를 입력받은 경우, 상기 (b1) 단계에서 저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환하는 것을 특징으로 하는 것을 특징으로 하는 가변 폭 데이터 패킷 암호화 방법.

【청구항 29】

(a) 복호화 과정에서 처리되는 암호화 데이터 패킷의 폭인 고정 폭이, 임의의 인터페이스 모듈로부터 입력되는 임의의 암호화 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합하여, 상기 고정 폭의 암호화 데이터 패킷을 생성하여 출력하는 단계; 및

(b) 상기 (a) 단계에서 출력된 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 고정 폭의 데이터 패킷을 생성하여 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 30】

제 29 항에 있어서,

(c) 상기 (b) 단계에서 출력된 고정 폭의 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 데이터 패킷을 생성하고, 상기 생성된 결합 값의 개수의 가변 폭의 데이터 패킷을 차례로 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 31】

제 29 항에 있어서,

상기 (a) 단계는 상기 가변 폭이 상기 고정 폭의 배수인 경우, 상기 가변 폭의 암호화 데이터 패킷을 입력받고, 상기 입력된 가변 폭의 암호화 데이터 패킷을 상기 가변 폭을 상기 고정 폭으로 나눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 생성하여 차례로 출력하고,

상기 (b) 단계는 상기 (a) 단계에서 출력된 분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 복호화하여, 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 32】

제 31 항에 있어서, 상기 (a) 단계는 상기 (b) 단계에서 출력된 상기 분리 값의 개수의 고정 폭의 데이터 패킷을 차례로 입력받고, 상기 차례로 입력된 분리 값의 개수의 고정 폭의 데이터 패킷을 결합하여, 상기 가변 폭의 데이터 패킷을 생성하여 출력하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 33】

제 29 항에 있어서, 상기 (b) 단계는

(b1) 상기 (a) 단계에서 생성된 고정 폭의 암호화 데이터 패킷을 저장하는 단계;

(b2) 상기 (b1) 단계에서 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환하는 단계;

(b3) 상기 (b2) 단계에서 변환된 복호화 폭의 암호화 데이터를 복호화하여, 상기 복호화 폭의 데이터를 생성하는 단계;

(b4) 상기 (b3) 단계에서 생성된 복호화 폭의 데이터를 상기 고정 폭의 데이터 패킷으로 변환하는 단계; 및

(b5) 상기 (b4) 단계에서 변환된 고정 폭의 데이터 패킷을 저장하는 단계를 포함하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 34】

제 33 항에 있어서,

상기 (b3) 단계는 상기 복호화 폭의 데이터가 생성된 경우, 복호화 완료 신호를 생성하여 출력하고,

(b6) 상기 (b3) 단계에서 출력된 복호화 완료 신호를 입력받은 경우, 고정 폭-복호화 폭 변환 신호를 생성하여 출력하는 단계를 포함하고,

상기 (b2) 단계는 상기 (b6) 단계에서 출력된 고정 폭-복호화 폭 변환 신호를 입력받은 경우, 상기 (b1) 단계에서 저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환하는 것을 특징으로 하는 가변 폭 암호화 데이터 패킷 복호화 방법.

【청구항 35】

(a) 시스템 내부에서 처리되는 데이터 패킷의 폭인 고정 폭이, 외부로부터 입력되는 임의의 데이터 패킷의 폭인 가변 폭의 배수인 경우, 상기 고정 폭을 상기 가변 폭으로 나눈 값인 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력받는 단계;

(b) 상기 (a) 단계에서 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합하여, 상기 고정 폭의 제 1 데이터 패킷을 생성하는 단계; 및

(c) 상기 (b1) 단계에서 생성된 고정 폭의 제 1 데이터 패킷을 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 36】

제 35 항에 있어서, 상기 (b) 단계는

(b1) 상기 (a) 단계에서 차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 저장하는 단계; 및

(b2) 상기 (b1) 단계에서 차례로 저장된 결합 값의 개수의 가변 폭의 데이터 패킷을 결합하여, 상기 고정 폭의 제 1 데이터 패킷을 생성하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 37】

제 36 항에 있어서, 상기 (b) 단계는

(b3) 상기 결합 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 상기 생성된 결합 신호를 출력하는 단계를 포함하고,

상기 (b2) 단계는 상기 (b3) 단계에서 출력된 결합 신호를 입력받을 때마다, 상기 저장된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 결합하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 38】

제 35 항에 있어서,

(d) 상기 고정 폭의 제 2 데이터 패킷을 입력받는 단계;

(e) 상기 (d) 단계에서 입력된 고정 폭의 제 2 데이터 패킷을 상기 결합 값의 개수로 분리하여, 상기 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 생성하는 단계; 및

(f) 상기 (e) 단계에서 생성된 결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 39】

제 35 항에 있어서,

(g) 상기 가변 폭이 상기 고정 폭의 배수인 경우, 가변 폭의 제 1 데이터 패킷을 입력받는 단계;

(h) 상기 (g) 단계에서 입력된 가변 폭의 제 1 데이터 패킷을 상기 가변 폭을 상기 고정 폭로 나눈 값인 분리 값의 개수로 분리하여, 상기 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 생성하는 단계; 및

(i) 상기 (h) 단계에서 생성된 분리 값의 개수의 고정 폭의 제 1 데이터 패킷을 차례로 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 40】

제 35 항에 있어서,

(j) 상기 가변 폭을 상기 고정 폭으로 나눈 값인, 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력받는 단계;

(k) 상기 (j) 단계에서 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합하여, 상기 가변 폭의 제 2 데이터 패킷을 생성하는 단계; 및

(l) 상기 (k) 단계에서 생성된 가변 폭의 제 2 데이터 패킷을 출력하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 41】

제 40 항에 있어서, 상기 (k) 단계는

(k1) 상기 (j) 단계에서 차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 저장하는 단계; 및

(k2) 상기 (k1) 단계에서 차례로 저장된 고정 폭의 제 2 데이터 패킷을 결합하여, 상기 가변 폭의 제 2 데이터 패킷을 생성하는 단계를 포함하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 42】

제 41 항에 있어서, 상기 (k) 단계는

(k3) 상기 분리 값으로부터 1을 뺀 값을 카운트하고, 카운트할 때마다 결합 신호를 생성하고, 상기 생성된 결합 신호를 출력하는 단계를 포함하고,

상기 (k2) 단계는 상기 (k3) 단계에서 출력된 결합 신호를 입력받을 때마다, 상기 저장된 결합 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 결합하는 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 43】

제 38 항 또는 제 42 항에 있어서, 상기 제 2 데이터 패킷은 상기 제 1 데이터 패킷으로부터 암호화된 데이터 패킷인 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 44】

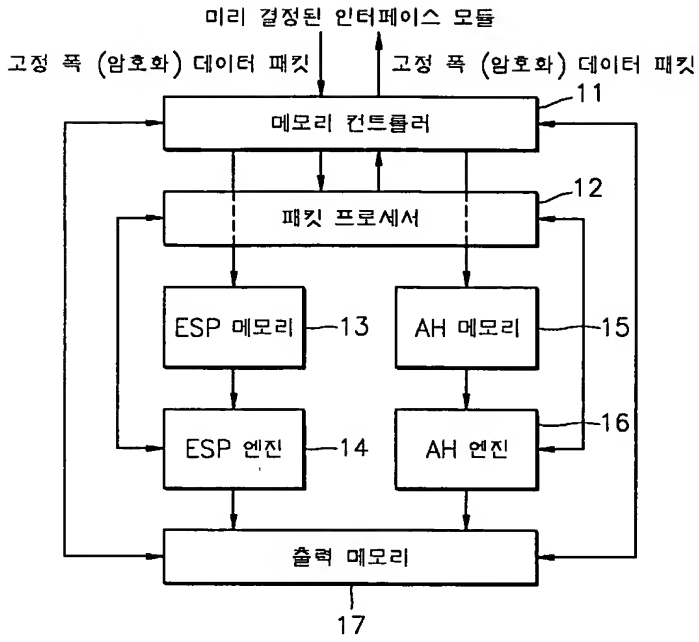
제 38 항 또는 제 42 항에 있어서, 상기 제 2 데이터 패킷은 상기 제 1 데이터 패킷으로부터 복호화된 데이터 패킷인 것을 특징으로 하는 가변 폭-고정 폭 데이터 패킷 변환 방법.

【청구항 45】

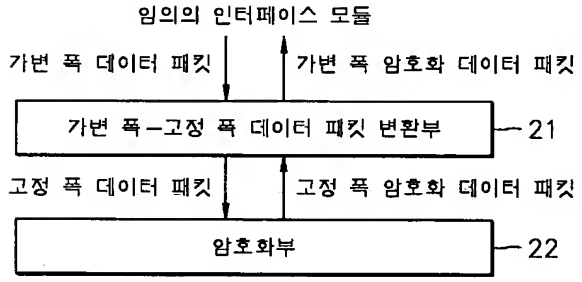
제 23 항 내지 제 44 항 중에 어느 한 항의 방법을 컴퓨터에서 실행시키기 위한 프로그램을 기록한 컴퓨터로 읽을 수 있는 기록매체.

【도면】

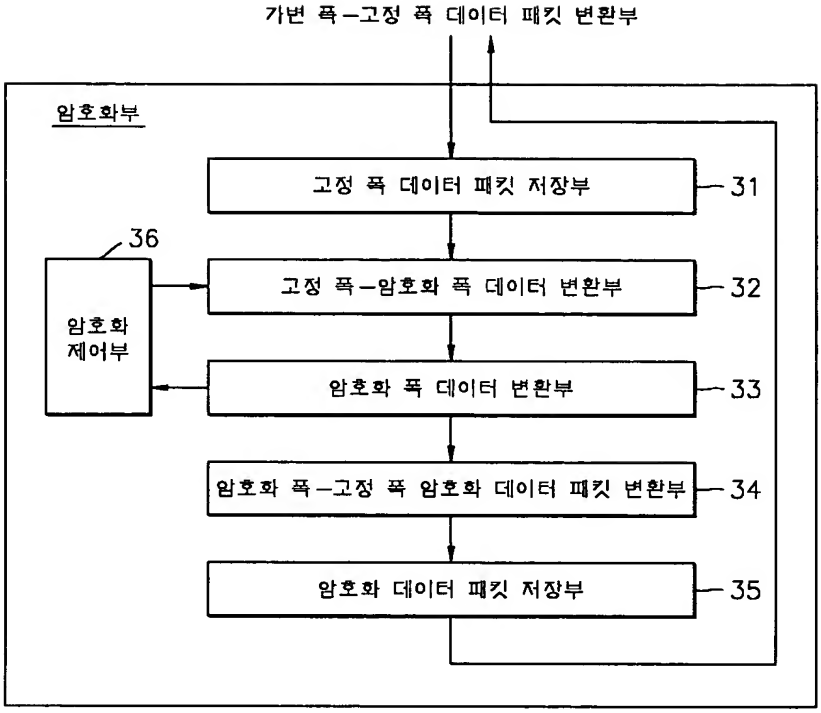
【도 1】


미리 결정된 인터페이스 모듈
고정 폭 (암호화) 데이터 패킷
고정 폭 (암호화) 데이터 패킷
메모리 컨트롤러
11
패킷 프로세서
12
ESP 메모리
13
AH 메모리
15
ESP 엔진
14
AH 엔진
16
출력 메모리
17

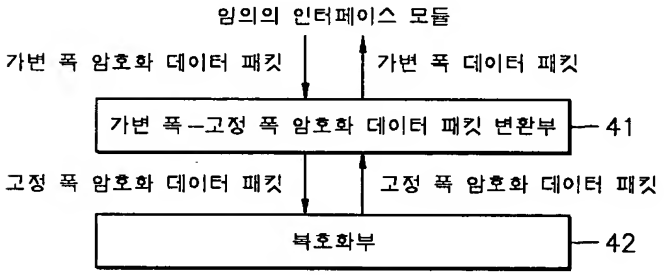
【도 2】


임의의 인터페이스 모듈
가변 폭 데이터 패킷
가변 폭 암호화 데이터 패킷
가변 폭-고정 폭 데이터 패킷 변환부
21
고정 폭 데이터 패킷
고정 폭 암호화 데이터 패킷
암호화부
22

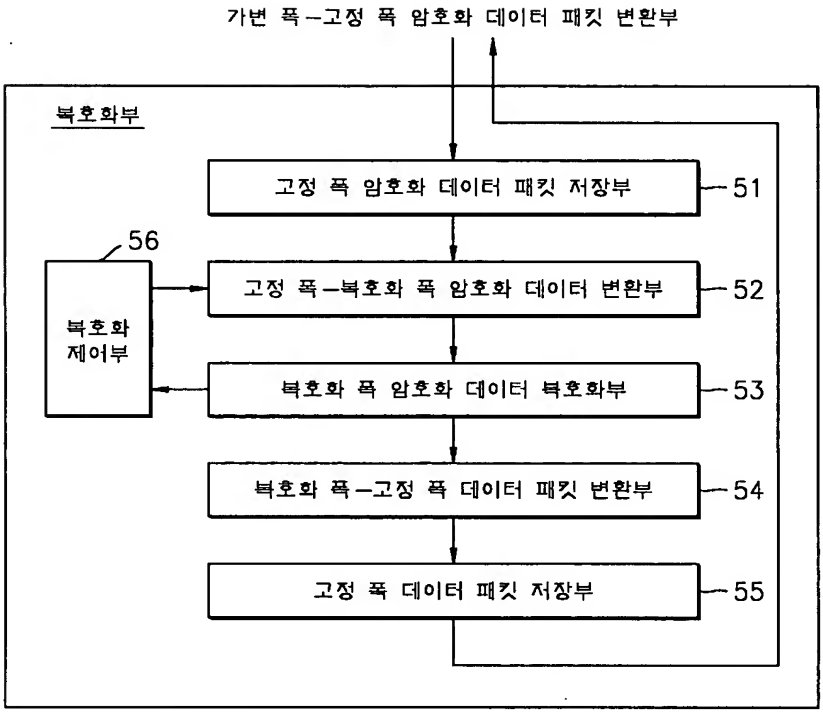
【도 3】


가변 폭-고정 폭 데이터 패킷 변환부
암호화부
고정 폭 데이터 패킷 저장부
31
36
암호화 제어부
고정 폭-암호화 폭 데이터 변환부
32
암호화 폭 데이터 변환부
33
암호화 폭-고정 폭 암호화 데이터 패킷 변환부
34
암호화 데이터 패킷 저장부
35

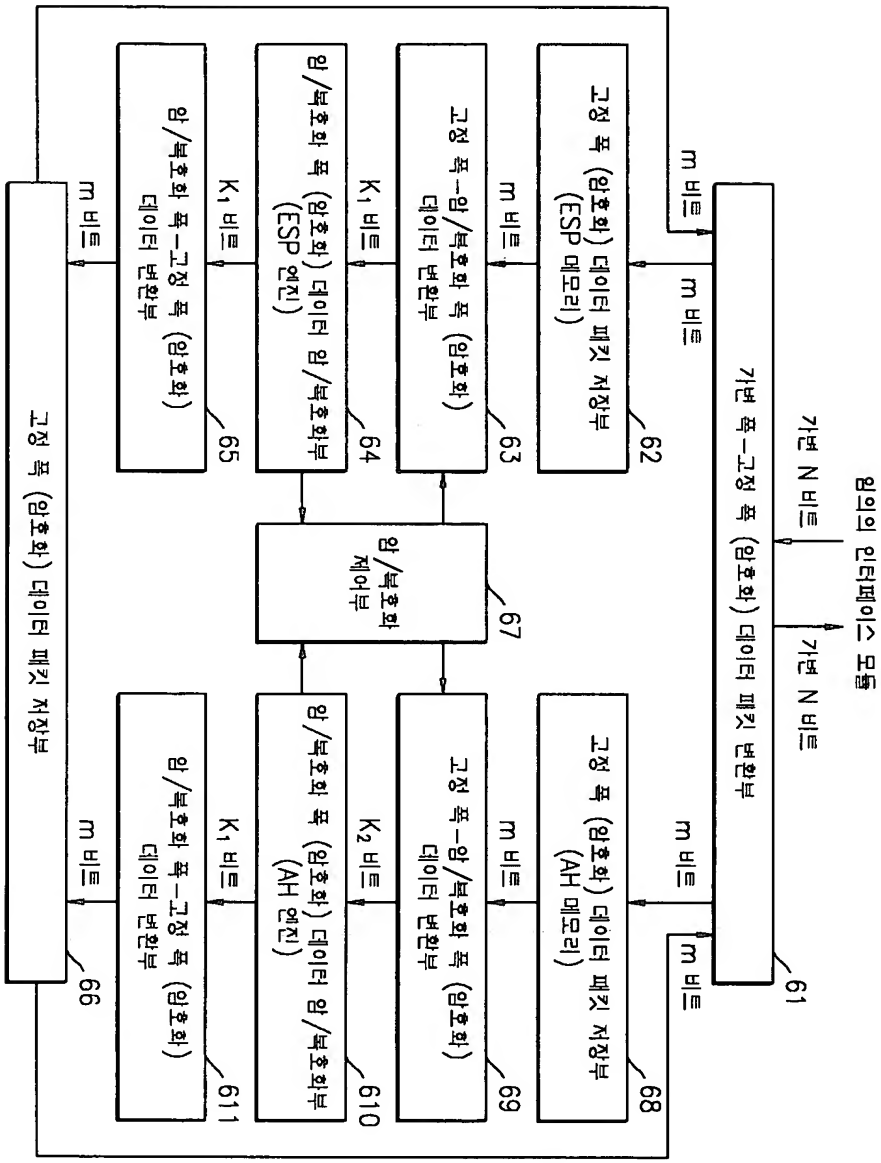
【도 4】


임의의 인터페이스 모듈
가변 폭 암호화 데이터 패킷
가변 폭 데이터 패킷
가변 폭-고정 폭 암호화 데이터 패킷 변환부
41
고정 폭 암호화 데이터 패킷
고정 폭 암호화 데이터 패킷
복호화부
42

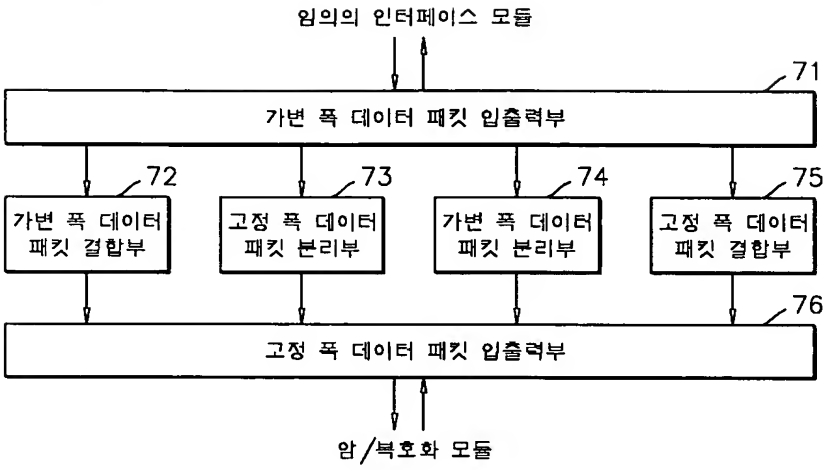
【도 5】


가변 폭-고정 폭 암호화 데이터 패킷 변환부
복호화부
고정 폭 암호화 데이터 패킷 저장부
51
56
복호화 제어부
고정 폭-복호화 폭 암호화 데이터 변환부
52
복호화 폭 암호화 데이터 복호화부
53
복호화 폭-고정 폭 데이터 패킷 변환부
54
고정 폭 데이터 패킷 저장부
55

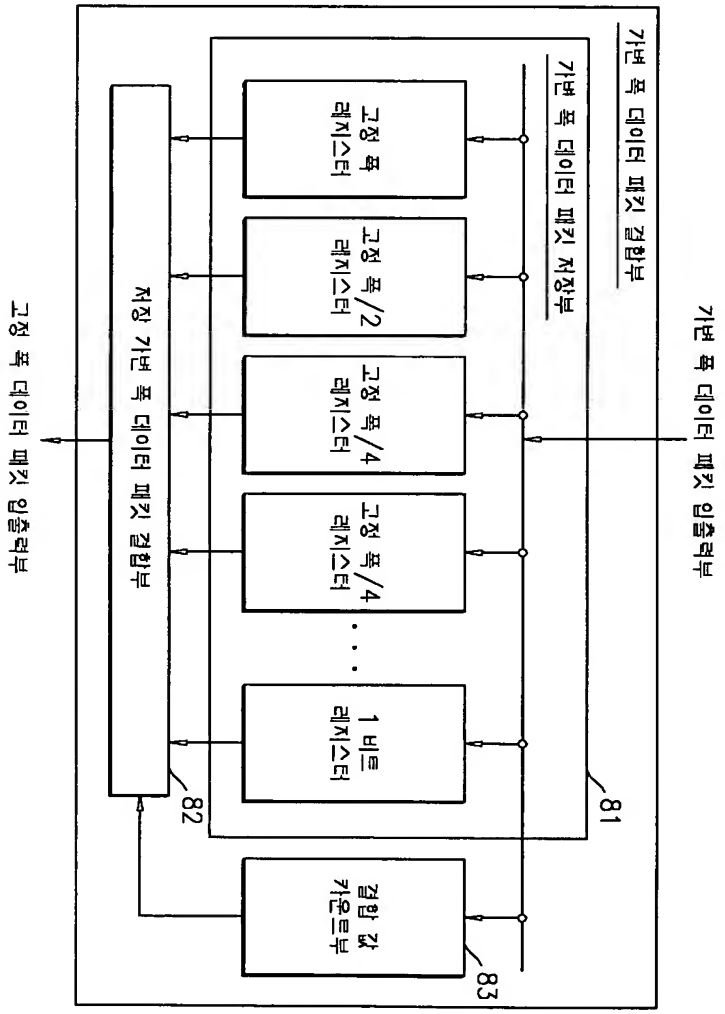
【도 6】


임의의 인터페이스 모듈
가변 N 비트
가변 N 비트
가변 폭-고정 폭 (암호화) 데이터 패킷 변환부
61
m 비트
m 비트
고정 폭 (암호화) 데이터 패킷 저장부
68
고정 폭 (암호화) 데이터 패킷 저장부
62
m 비트
m 비트
고정 폭-암/복호화 폭 (암호화) 데이터 변환부
69
고정 폭-암/복호화 폭 (암호화) 데이터 변환부
63
m 비트
m 비트
암/복호화 폭 (암호화) 데이터 암/복호화부
610
암/복호화 폭 (암호화) 데이터 암/복호화부
64
K2 비트
K1 비트
암/복호화 폭-고정 폭 (암호화) 데이터 변환부
611
암/복호화 폭-고정 폭 (암호화) 데이터 변환부
65
K1 비트
K1 비트
암/복호화 제어부
67
m 비트
m 비트
고정 폭 (암호화) 데이터 패킷 저장부
66

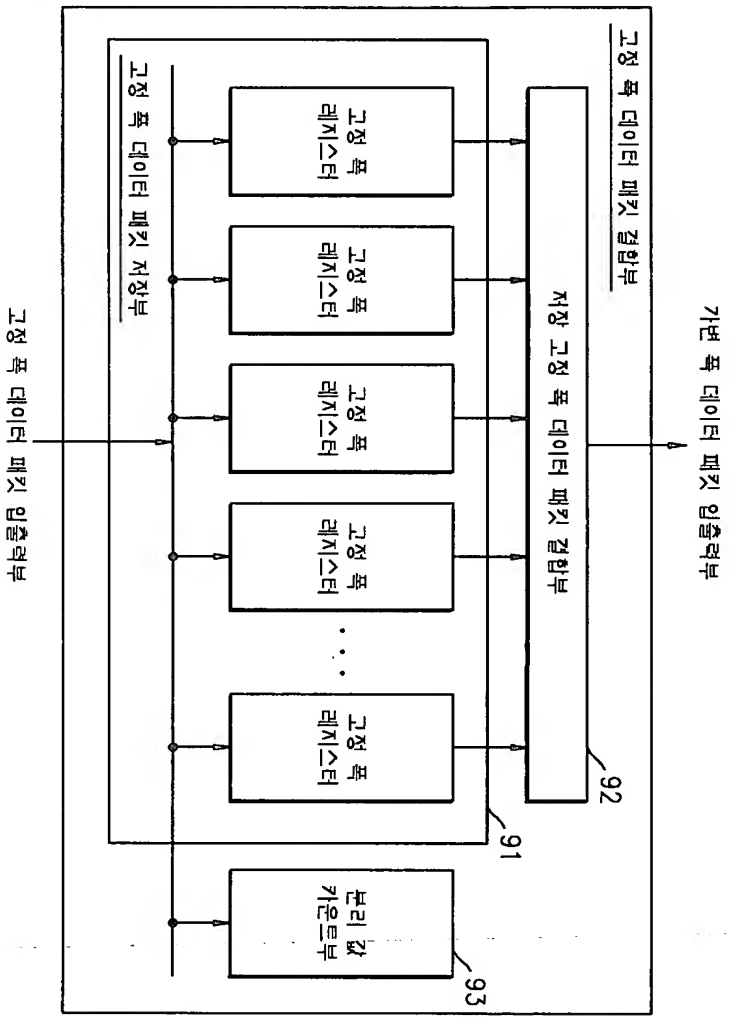
【도 7】


임의의 인터페이스 모듈
71
가변 폭 데이터 패킷 입출력부
72
73
74
75
가변 폭 데이터 패킷 결합부
고정 폭 데이터 패킷 분리부
가변 폭 데이터 패킷 분리부
고정 폭 데이터 패킷 결합부
76
고정 폭 데이터 패킷 입출력부
암/복호화 모듈

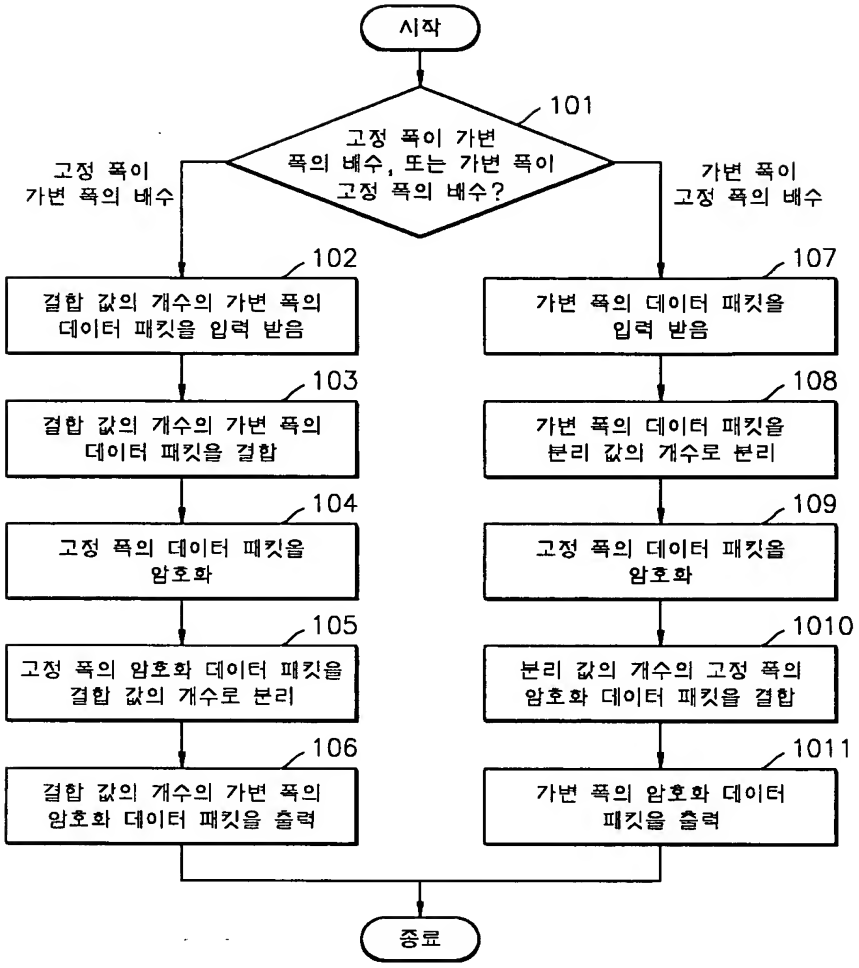
【도 8】


가변 폭 데이터 패킷 결합부
가변 폭 데이터 패킷 저장부
고정 폭 레지스터
고정 폭/2 레지스터
고정 폭/4 레지스터
고정 폭/4 레지스터
1 비트 레지스터
결합 값 카운트부
저장 가변 폭 데이터 패킷 결합부
82
81
83
고정 폭 데이터 패킷 입출력부
가변 폭 데이터 패킷 입출력부

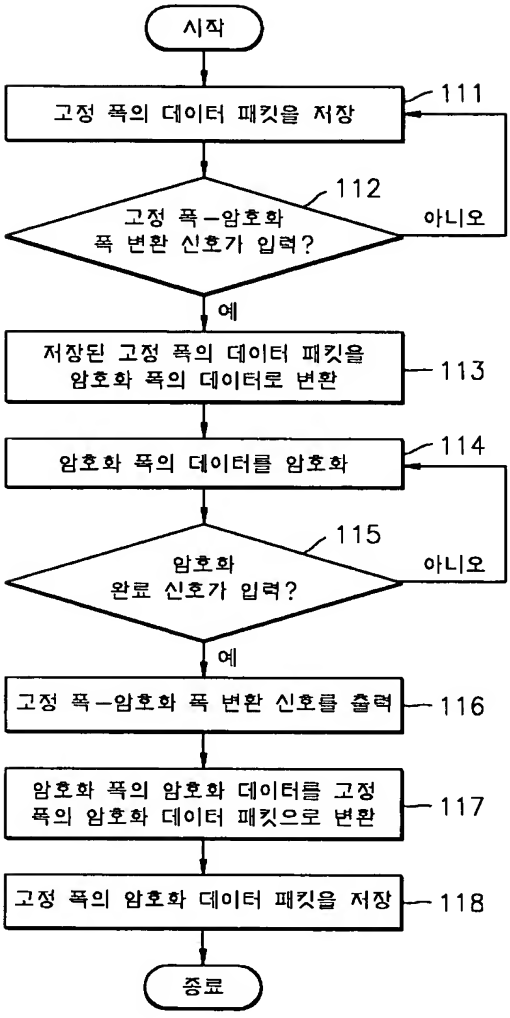
【도 9】


고정 폭 데이터 패킷 입출력부
고정 폭 데이터 패킷 저장부
고정 폭 레지스터
고정 폭 레지스터
고정 폭 레지스터
고정 폭 레지스터
고정 폭 레지스터
91
고정 폭 데이터 패킷 결합부
저장 고정 폭 데이터 패킷 결합부
92
가변 폭 데이터 패킷 입출력부
남은 값 카운트부
93

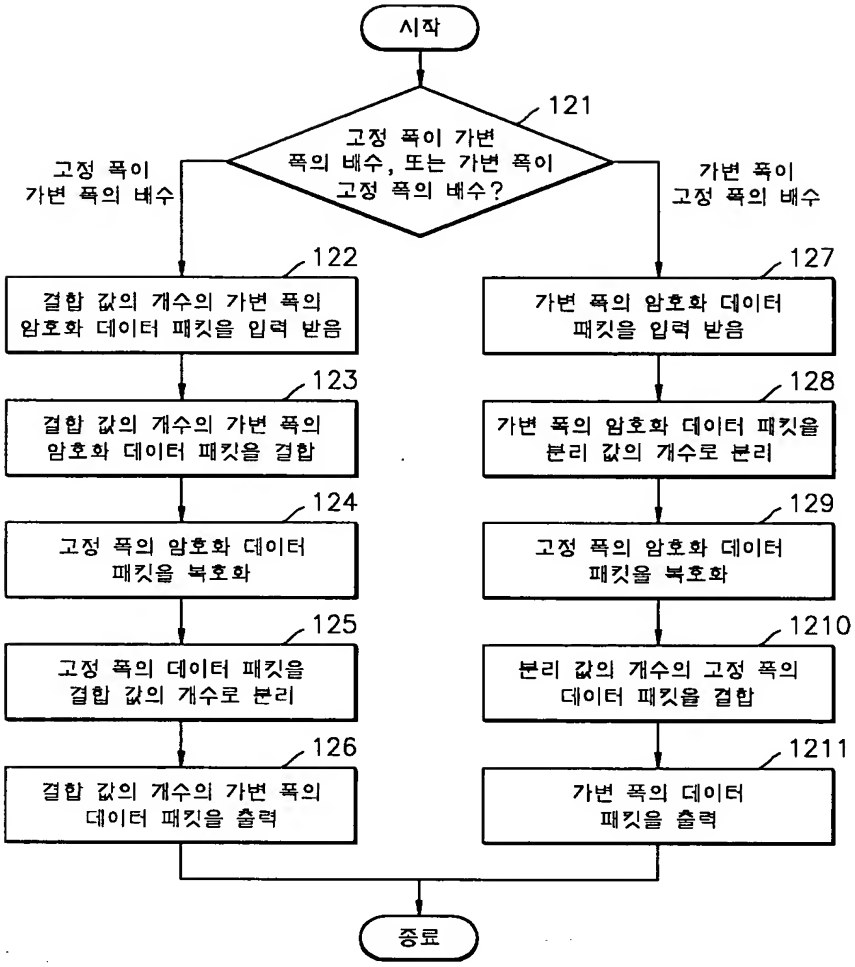
【도 10】


시작
101
고정 폭이 가변 폭의 배수, 또는 가변 폭이 고정 폭의 배수?
고정 폭이 가변 폭의 배수
가변 폭이 고정 폭의 배수
102
결합 값의 개수의 가변 폭의 데이터 패킷을 입력 받음
103
결합 값의 개수의 가변 폭의 데이터 패킷을 결합
104
고정 폭의 데이터 패킷을 암호화
105
고정 폭의 암호화 데이터 패킷을 결합 값의 개수로 분리
106
결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 출력
107
가변 폭의 데이터 패킷을 입력 받음
108
가변 폭의 데이터 패킷을 분리 값의 개수로 분리
109
고정 폭의 데이터 패킷을 암호화
1010
분리 값의 개수의 고정 폭의 암호화 데이터 패킷을 결합
1011
가변 폭의 암호화 데이터 패킷을 출력
종료

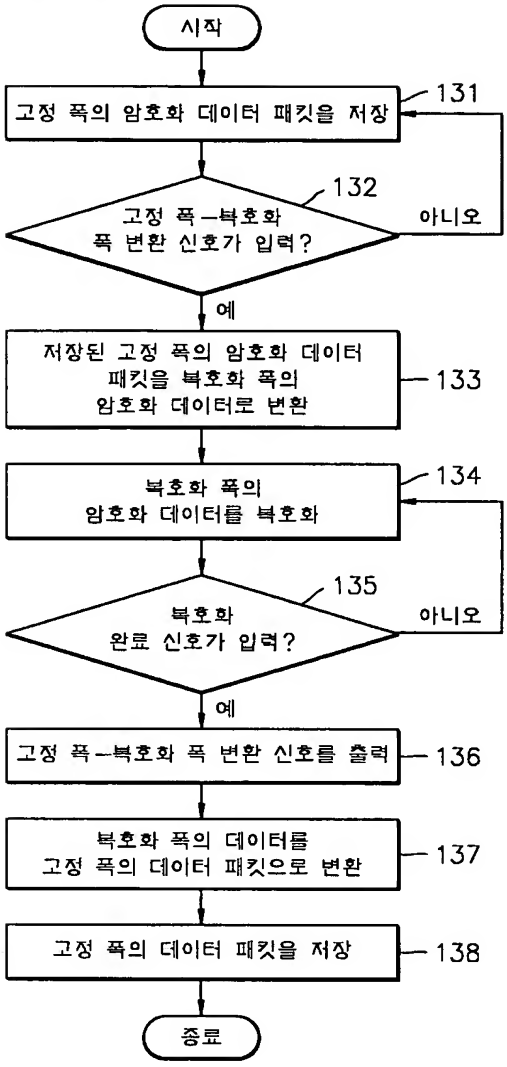
【도 11】


시작
고정 폭의 데이터 패킷을 저장
111
고정 폭-암호화 폭 변환 신호가 입력?
112
아니오
예
저장된 고정 폭의 데이터 패킷을 암호화 폭의 데이터로 변환
113
암호화 폭의 데이터를 암호화
114
암호화 완료 신호가 입력?
115
아니오
예
고정 폭-암호화 폭 변환 신호를 출력
116
암호화 폭의 암호화 데이터를 고정 폭의 암호화 데이터 패킷으로 변환
117
고정 폭의 암호화 데이터 패킷을 저장
118
종료

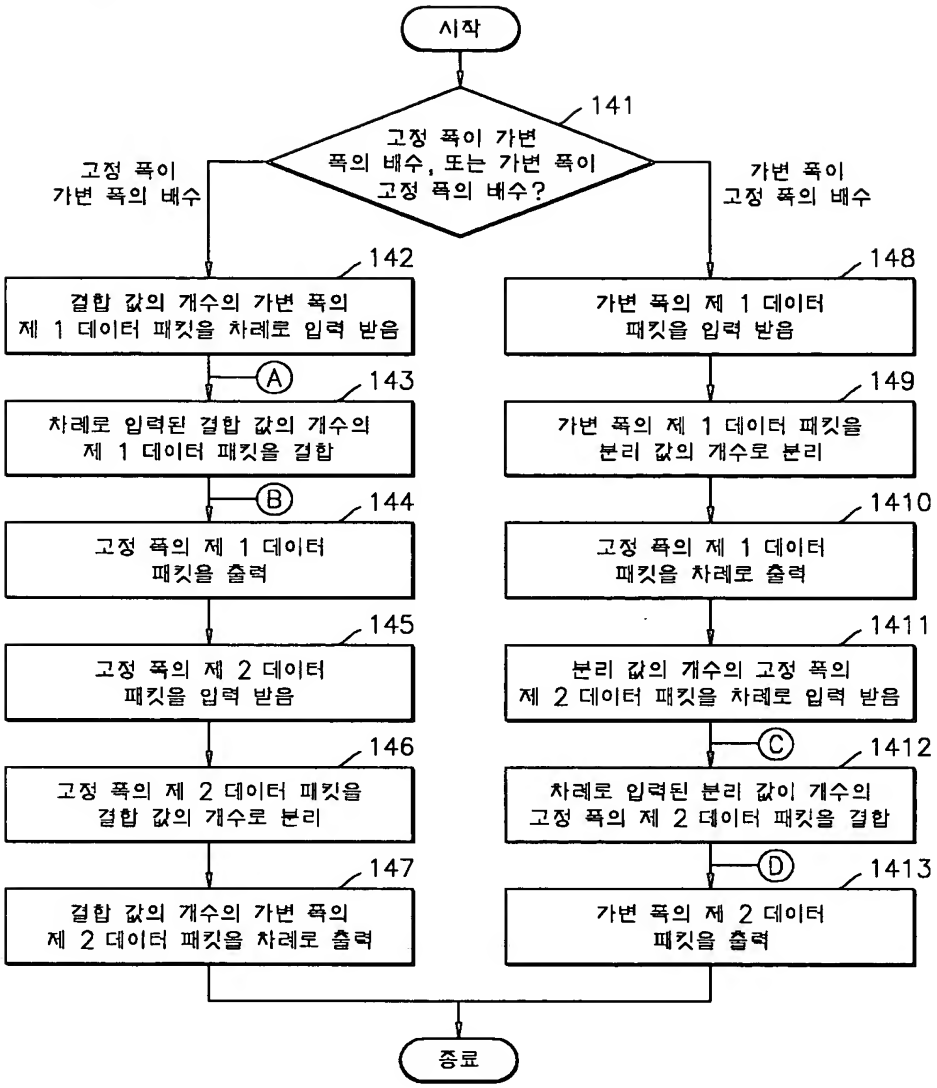
【도 12】


시작
121
고정 폭이 가변 폭의 배수, 또는 가변 폭이 고정 폭의 배수?
고정 폭이 가변 폭의 배수
가변 폭이 고정 폭의 배수
122
결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 입력 받음
123
결합 값의 개수의 가변 폭의 암호화 데이터 패킷을 결합
124
고정 폭의 암호화 데이터 패킷을 복호화
125
고정 폭의 데이터 패킷을 결합 값의 개수로 분리
126
결합 값의 개수의 가변 폭의 데이터 패킷을 출력
127
가변 폭의 암호화 데이터 패킷을 입력 받음
128
가변 폭의 암호화 데이터 패킷을 분리 값의 개수로 분리
129
고정 폭의 암호화 데이터 패킷을 복호화
1210
분리 값의 개수의 고정 폭의 데이터 패킷을 결합
1211
가변 폭의 데이터 패킷을 출력
종료

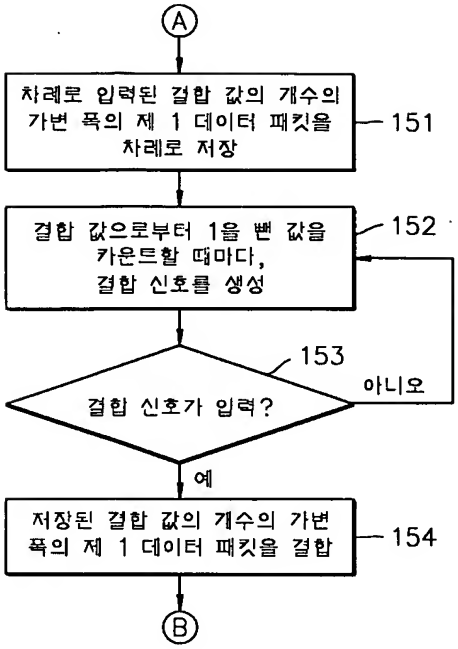
【도 13】


시작
고정 폭의 암호화 데이터 패킷을 저장
131
고정 폭-복호화 폭 변환 신호가 입력?
132
아니오
예
저장된 고정 폭의 암호화 데이터 패킷을 복호화 폭의 암호화 데이터로 변환
133
복호화 폭의 암호화 데이터를 복호화
134
복호화 완료 신호가 입력?
135
아니오
예
고정 폭-복호화 폭 변환 신호를 출력
136
복호화 폭의 데이터를 고정 폭의 데이터 패킷으로 변환
137
고정 폭의 데이터 패킷을 저장
138
종료

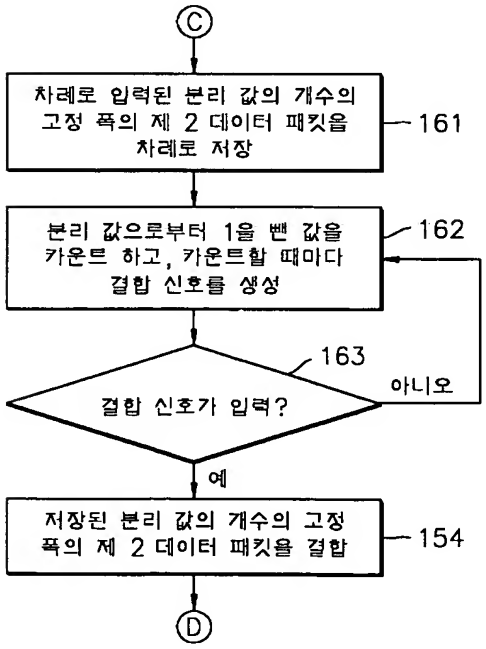
【도 14】


시작
141
고정 폭이 가변 폭의 배수, 또는 가변 폭이 고정 폭의 배수?
고정 폭이 가변 폭의 배수
가변 폭이 고정 폭의 배수
142
결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 입력 받음
A
143
차례로 입력된 결합 값의 개수의 제 1 데이터 패킷을 결합
B
144
고정 폭의 제 1 데이터 패킷을 출력
145
고정 폭의 제 2 데이터 패킷을 입력 받음
146
고정 폭의 제 2 데이터 패킷을 결합 값의 개수로 분리
147
결합 값의 개수의 가변 폭의 제 2 데이터 패킷을 차례로 출력
148
가변 폭의 제 1 데이터 패킷을 입력 받음
149
가변 폭의 제 1 데이터 패킷을 분리 값의 개수로 분리
1410
고정 폭의 제 1 데이터 패킷을 차례로 출력
1411
분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 입력 받음
C
1412
차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합
D
1413
가변 폭의 제 2 데이터 패킷을 출력
종료

【도 15】


A
차례로 입력된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 차례로 저장
151
결합 값으로부터 1을 뺀 값을 카운트할 때마다, 결합 신호를 생성
152
153
결합 신호가 입력?
아니오
예
저장된 결합 값의 개수의 가변 폭의 제 1 데이터 패킷을 결합
154
B

【도 16】


C
차례로 입력된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 차례로 저장
161
분리 값으로부터 1을 뺀 값을 카운트 하고, 카운트할 때마다 결합 신호를 생성
162
163
결합 신호가 입력?
아니오
예
저장된 분리 값의 개수의 고정 폭의 제 2 데이터 패킷을 결합
154
D